DualAuth

Smartphone-Based Physical Facility Access Control Technology

AutoPassword IoT Controller Product Introduction

01

Product Overview

02

Key Features

03

References

04

Contact

01 Product Overview

Smartphone-Based Physical Facility Access Control Technology

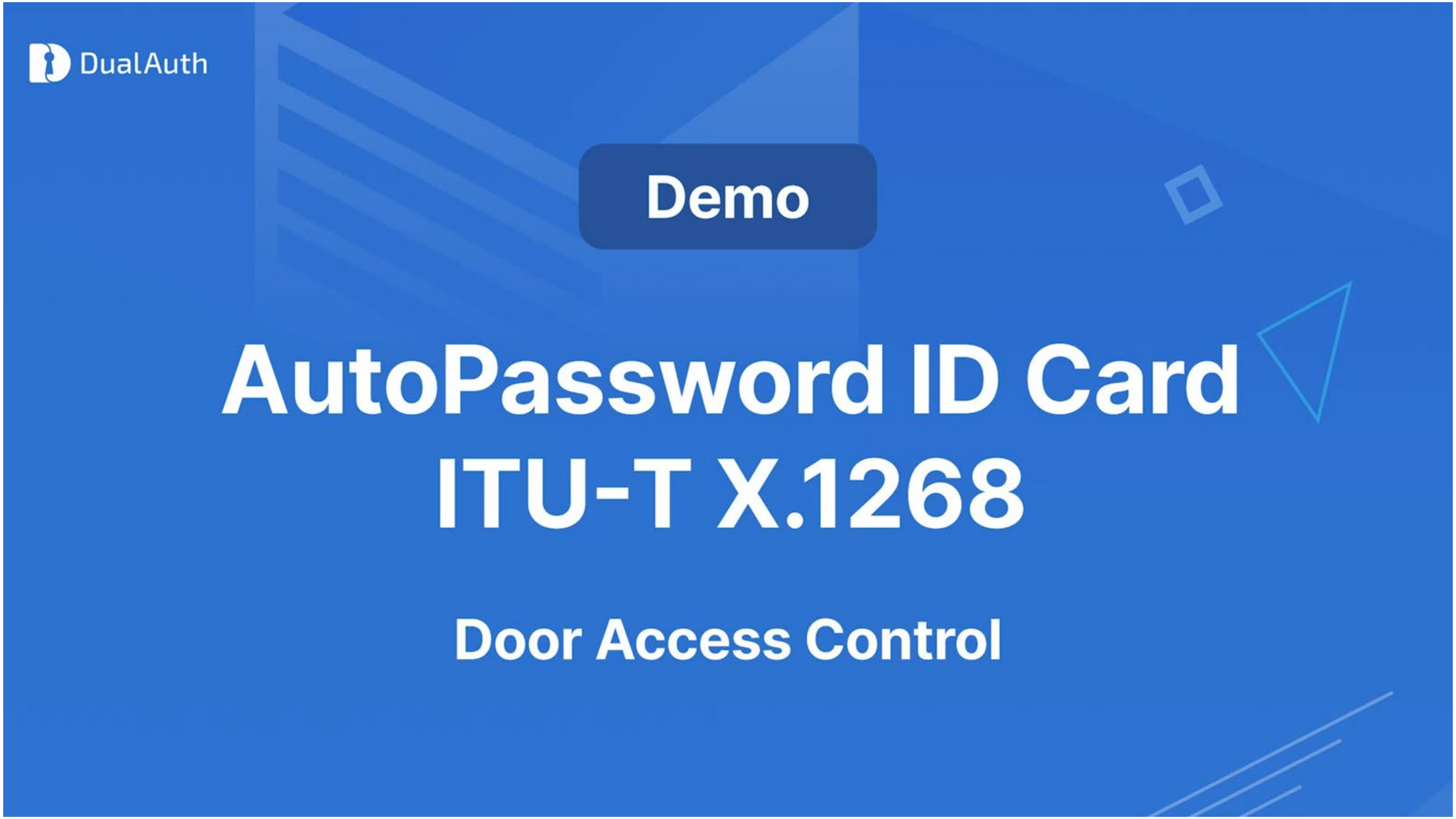
AutoPassword
IoT Controller

AutoPassword
ID Card

AutoPassword IoT Controller is a smartphone-based physical facility access control solution. It is designed to overcome the limitations of traditional methods where physical facilities directly collect and store users' biometric information, such as fingerprint or facial recognition devices.

This solution does not store user biometric information on the physical facility or server. It performs access requests solely through the biometric authentication function embedded in the user's smartphone. It controls access to physical facilities by transmitting only verified authentication values via a server-based mutual authentication structure. This technology is based on the international standard ITU-T X.1268.

01 Product Overview



DualAuth

Demo

AutoPassword ID Card

ITU-T X.1268

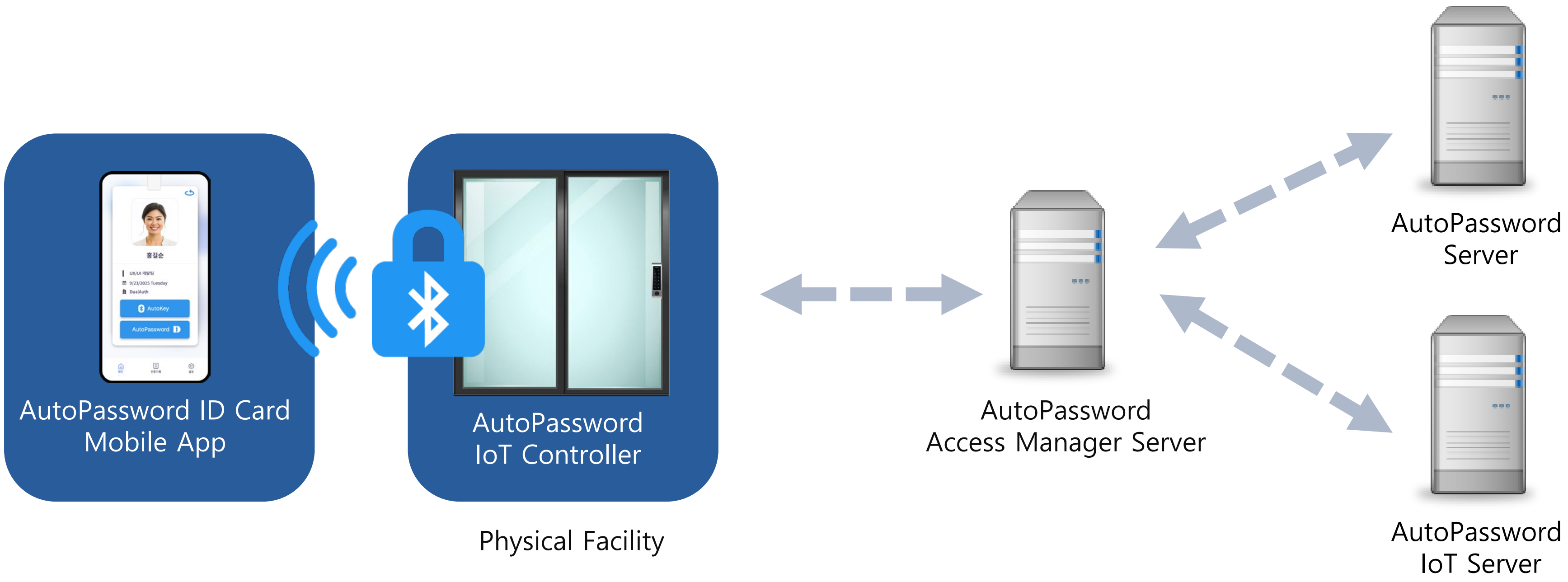
Door Access Control

https://youtu.be/S3favCBySLY

AutoPassword IoT Controller Architecture

To apply smartphone biometric authentication to physical facility access control, simply attach the AutoPassword IoT Controller to existing physical facilities, configure the AutoPassword Server and AutoPassword Access Manager Server, and distribute the AutoPassword ID Card mobile app to users.

The AutoPassword IoT Controller periodically transmits Bluetooth Low Energy (BLE) authentication beacons containing a facility identifier and a dynamic authentication value that changes every 60 seconds. This dynamic value fundamentally prevents replay attacks caused by fixed signal replication. Users can identify facilities only within the effective BLE range (approximately 10 meters). After selecting the identified facility on their smartphone, users confirm their intent to use the facility through biometric authentication. The AutoPassword server then verifies the request by validating the user’s authentication, access permissions, and facility information before activating the physical facility.



DualAuth

01

Product Overview

02

Key Features

03

References

04

Contact

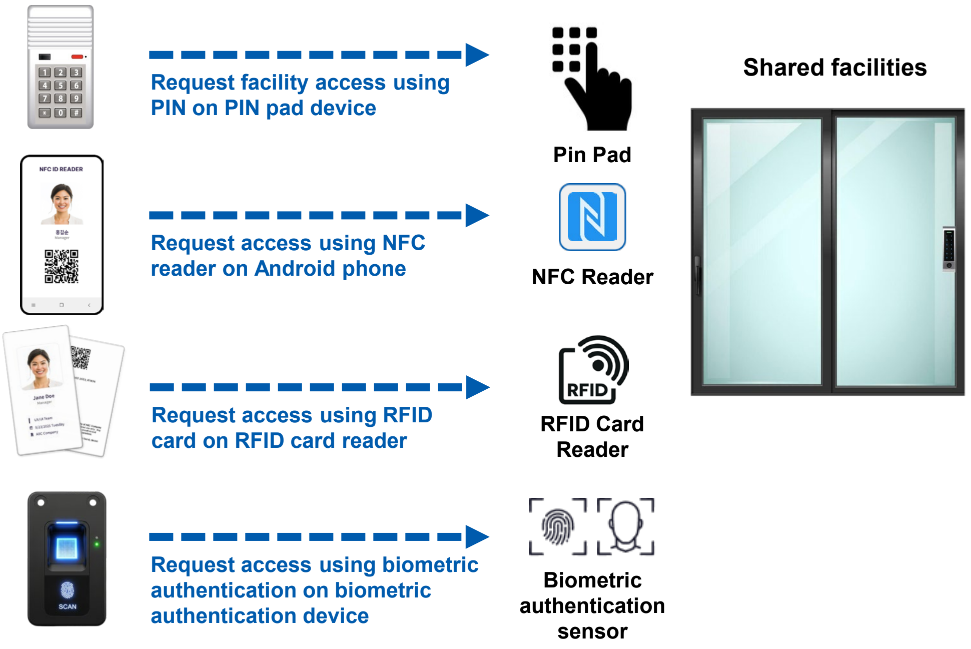
02 Key Features

Feature 1 – Smartphone-based access control technology optimized for shared facilities

Unlike personal IoT devices, shared facilities used by multiple users require high versatility and a standardized user experience. Shared passwords or access cards carry high risks of loss or theft and present limitations in user changes and management. Existing NFC card emulation methods only supported Android phones, restricting application in shared facilities for iPhone users.

AutoPassword ID Card operates identically on both iPhones and Android phones, providing a standardized user experience. It operates based on smartphone biometric authentication, making unauthorized use impossible. Furthermore, it can be installed as a ceiling-mounted unit, eliminating the need to expose a separate reader on exterior walls. This allows for use in apartment complexes, office buildings, and public facilities without compromising aesthetics.

Input-based facility access control technology



Request facility access using PIN on PIN pad device

Pin Pad

Request access using NFC reader on Android phone

NFC Reader

Request access using RFID card on RFID card reader

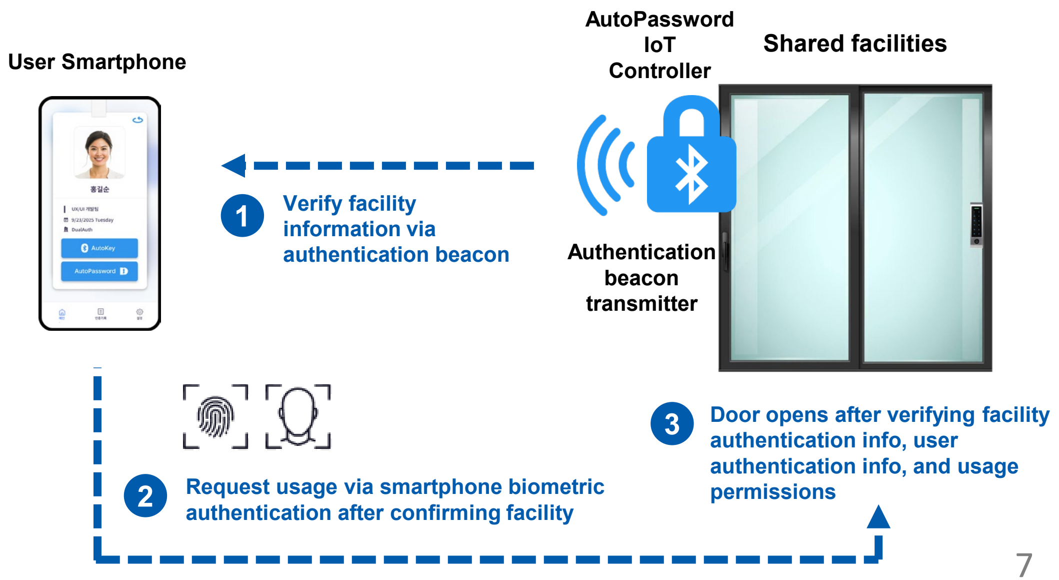
RFID Card Reader

Request access using biometric authentication on biometric authentication device

Biometric authentication sensor

Shared facilities

Output-based facility access control technology



User Smartphone

AutoPassword IoT Controller

Shared facilities

Authentication beacon transmitter

1 Verify facility information via authentication beacon

2 Request usage via smartphone biometric authentication after confirming facility

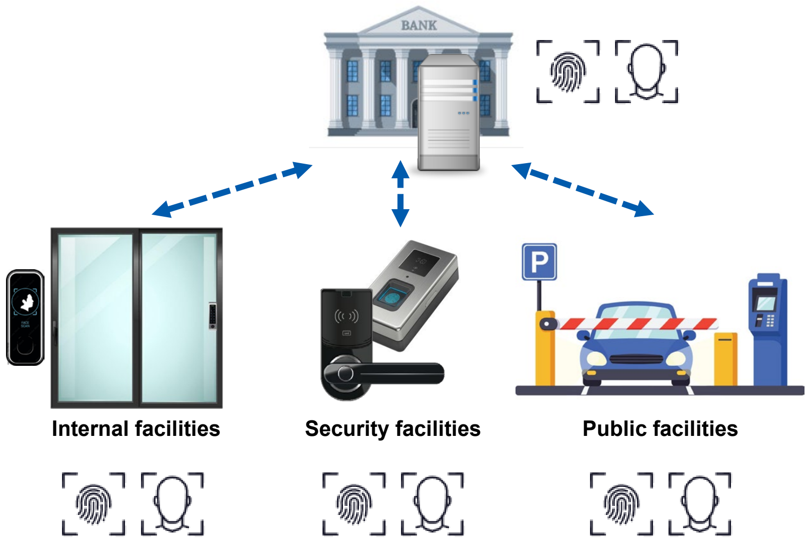
3 Door opens after verifying facility authentication info, user authentication info, and usage permissions

Feature 2 – Biometric Authentication without collecting personal biometric information

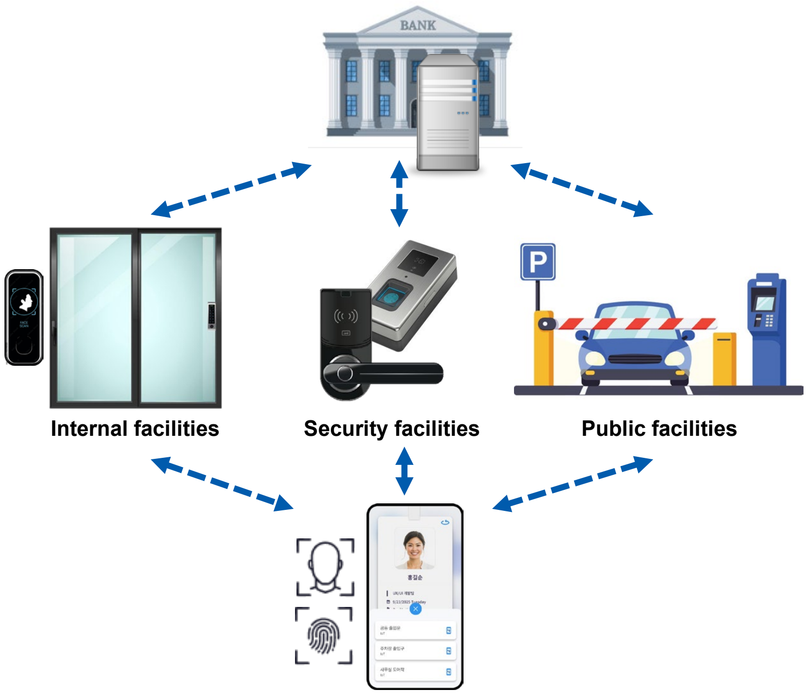
AutoPassword ID Card does not require users to directly input or register their biometric data at physical facilities. Instead, the physical facility transmits a BLE authentication beacon. The user then verifies the facility's authentication beacon via their smartphone and transmits the facility control command over the network using smartphone biometric authentication.

This out-of-band mutual authentication structure eliminates the need for separate biometric databases at each physical facility. User biometric data is stored and used exclusively within the individual's smartphone. This fundamentally eliminates the risk of privacy infringement.

On-site biometric authentication requiring
biometric information management at each facility



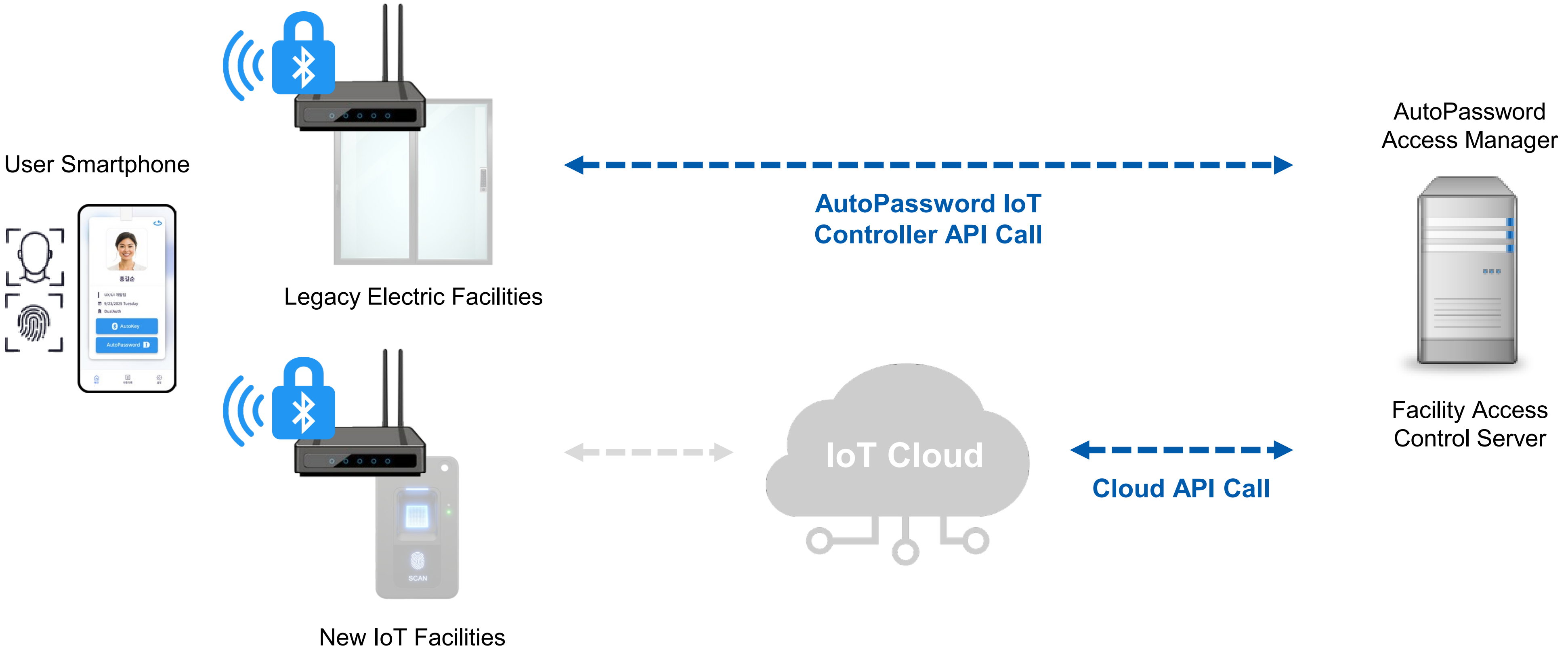
Off-site biometric authentication not requiring
biometric information management at each facility



Feature 3 – Convert legacy motorized facilities & personal IoT devices to shared IoT devices

The AutoPassword IoT Controller transforms legacy electric facilities in shared spaces—such as electric gates, light switches, and parking barriers—into public IoT devices controllable via smartphone.

Furthermore, even the latest IoT devices designed for personal use can be expanded for safe public deployment by installing the AutoPassword IoT Controller and integrating it with the device's cloud server via API.


User Smartphone
Legacy Electric Facilities
New IoT Facilities
AutoPassword IoT Controller API Call
IoT Cloud
Cloud API Call
AutoPassword Access Manager
Facility Access Control Server

Feature 4 – AutoPassword IoT Controller Detailed Specifications

The AutoPassword IoT Controller is an IoT control device that transmits authentication beacons and supports network APIs for communicating with the AutoPassword Access Manager server. This device provides 6 input ports for detecting the operational status of legacy motorized facilities and 6 output ports (I/O Ports) for transmitting control signals. It can be used to monitor the status and remotely control common motorized facilities such as automatic doors and parking barriers.

AutoPassword IoT Controller	
Model No	ES-MT1266
Manufacturer	eSTORM
Communication	Supports Wi-Fi 2.4 GHz and wired LAN communication
Power Supply	DC 5 V / 2 A
Control Voltage	≤ DC 12 V
Control Current	≤ 1 A
Switch Status Output	2-wire status detection
Detection Voltage	DC 3 V when switch is connected (ON)

01

Product Overview

02

Key Features

03

References

04

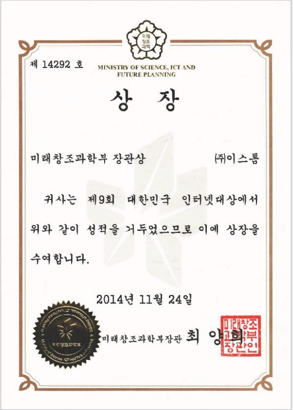
Contact

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
CWMA 건설근로자공제회 Construction Workers Mutual Aid Association	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 ㈜이스톰

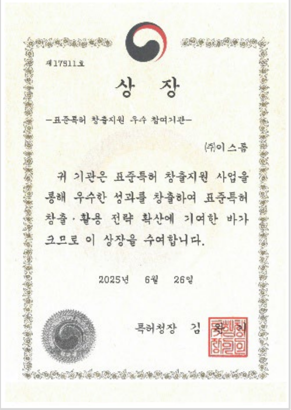
귀사는 제9회 대한민국 인터넷대상에서 위와 같이 성적을 거두었으므로 이에 상장을 수여합니다.

2014년 11월 24일

미래창조과학부장관 최 양 희

미래창조과학부장관인

The Korea Internet Awards



제17511호

상 장

–표준특허 창출지원 우수 참여기관–

㈜이스톰

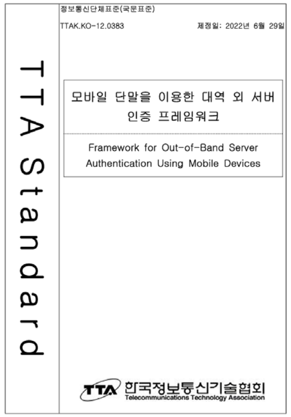
귀 기관은 표준특허 창출지원 사업을 통해 우수한 성과를 창출하여 표준특허 창출·활용 전략 확산에 기여한 바가 크므로 이 상장을 수여합니다.

2025년 6월 26일

특허청장 김 완 기

The Commissioner's Award

Standard Technologies



정보통신단체표준(국문표준)

TTAK.KO-12.0383 제정일: 2022년 6월 29일

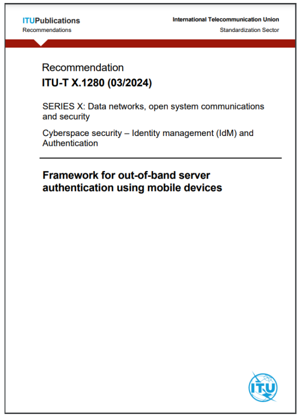
TTA Standard

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 UAF CERTIFIED

GOOD Software

ISO/IEC 25023, 25051, 25041

oath initiative for open authentication

IBM Security

NeP 신제품인증 NEW EXCELLENT PRODUCT

01

Product Overview

02

Key Features

03

References

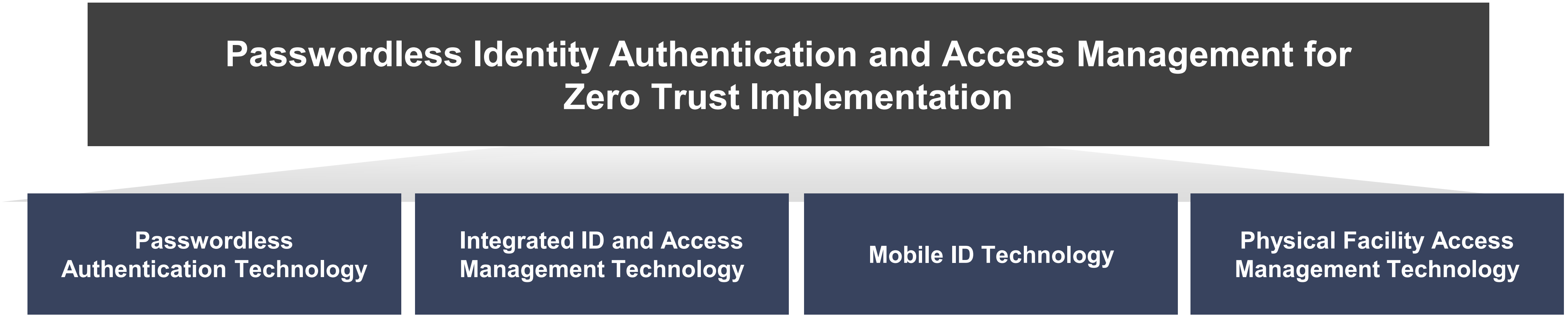
04

Contact

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.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

AutoPassword Access Manager

AutoPassword ID Card

AutoPassword ID Card Reader

AutoPassword ID Card

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