



Passwordless Technology for Zero Trust

AutoPassword

Product Introduction

01

Product Overview

02

Key Features

03

References

04

Contact

Passwordless Authentication Technology

AutoPassword



The passwordless solution AutoPassword is a mutual authentication technology in which the user does not enter a password, but instead the online system presents an AutoPassword to the user, and the user verifies the AutoPassword submitted by the online system using their smartphone. (International Standard X.1280)

01 Product Overview

The screenshot shows the homepage of Demo Bank. At the top, there is a navigation bar with the Demo Bank logo on the left and a 'Login' link on the right. Below the navigation bar, there are links for 'CHECKING', 'SAVINGS', 'CREDIT CARDS', 'HOME LOANS', and 'AUTO LOANS'. The main banner features a large image of a modern building with the Demo Bank logo in the center. Below the banner, there are three main service categories: 'Personal Banking', 'Credit Cards', and 'Corporate Banking'. The 'Banking Service' section includes 'SMART BANKING', 'EXCHANGE RATE', and 'CERTIFICATE CENTER'. The 'Financial Statement' section lists various reports with their dates. The 'Internet Banking FAQ' section has a plus sign icon. At the bottom, there are sections for 'LATEST NEWS' and 'SERVICE LINK'.

DEMO BANK

Login

CHECKING | SAVINGS | CREDIT CARDS | HOME LOANS | AUTO LOANS

DEMO BANK

Personal Banking | Credit Cards | Corporate Banking

Banking Service

- SMART BANKING
- EXCHANGE RATE
- CERTIFICATE CENTER

Financial Statement | Internet Banking FAQ +

2018 1Q Consolidated Financial Statements	18-08-01
2018 1Q Consolidated Financial Statements	18-08-01
2017 4Q Non-consolidated Financial Statements	18-08-01
2017 4Q Consolidated Financial Statements	18-08-01
2017 3Q Non-consolidated Financial Statements	18-08-01

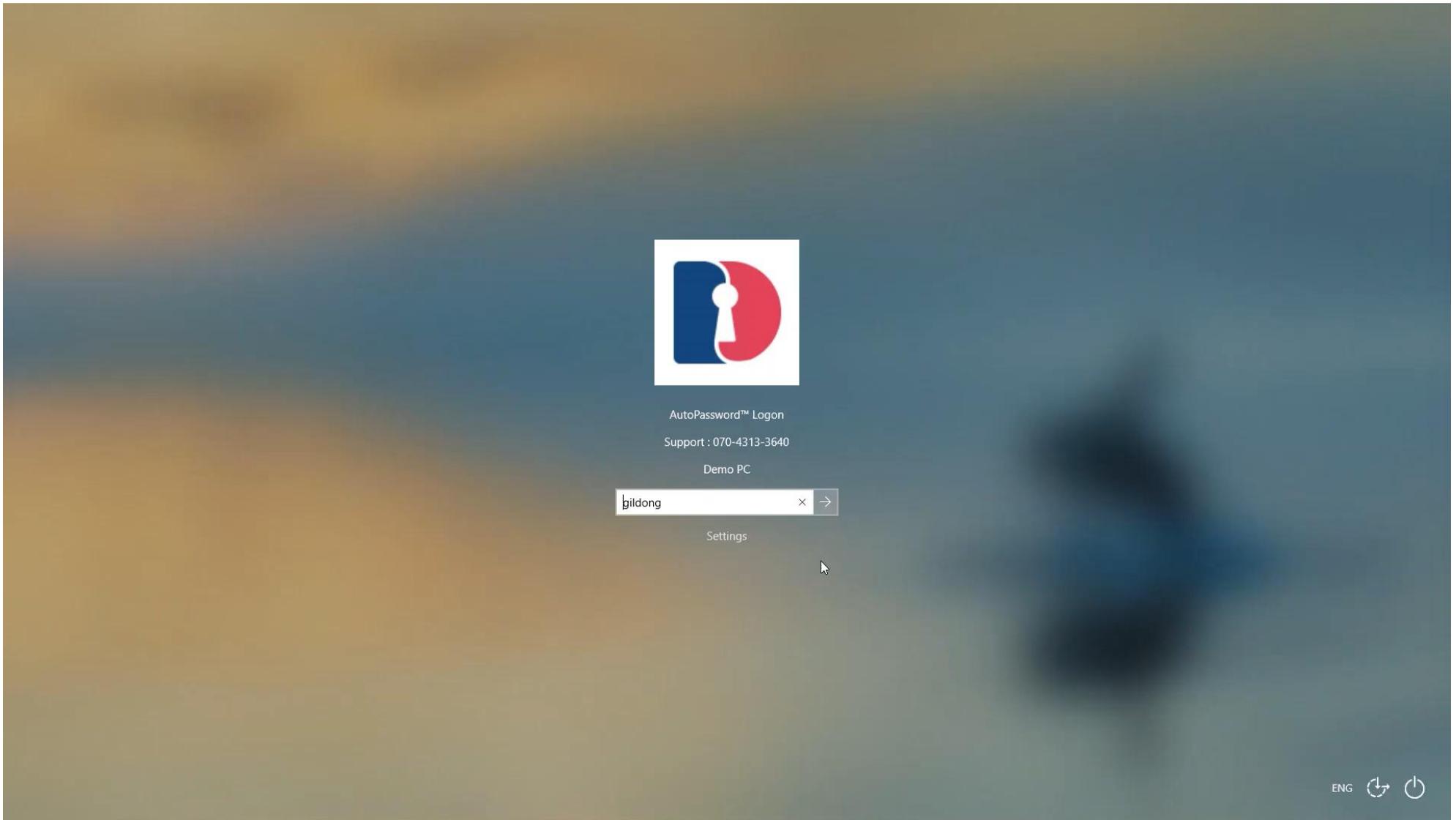
LATEST NEWS | **SERVICE LINK**

<https://youtu.be/ejT8qU36OMw>

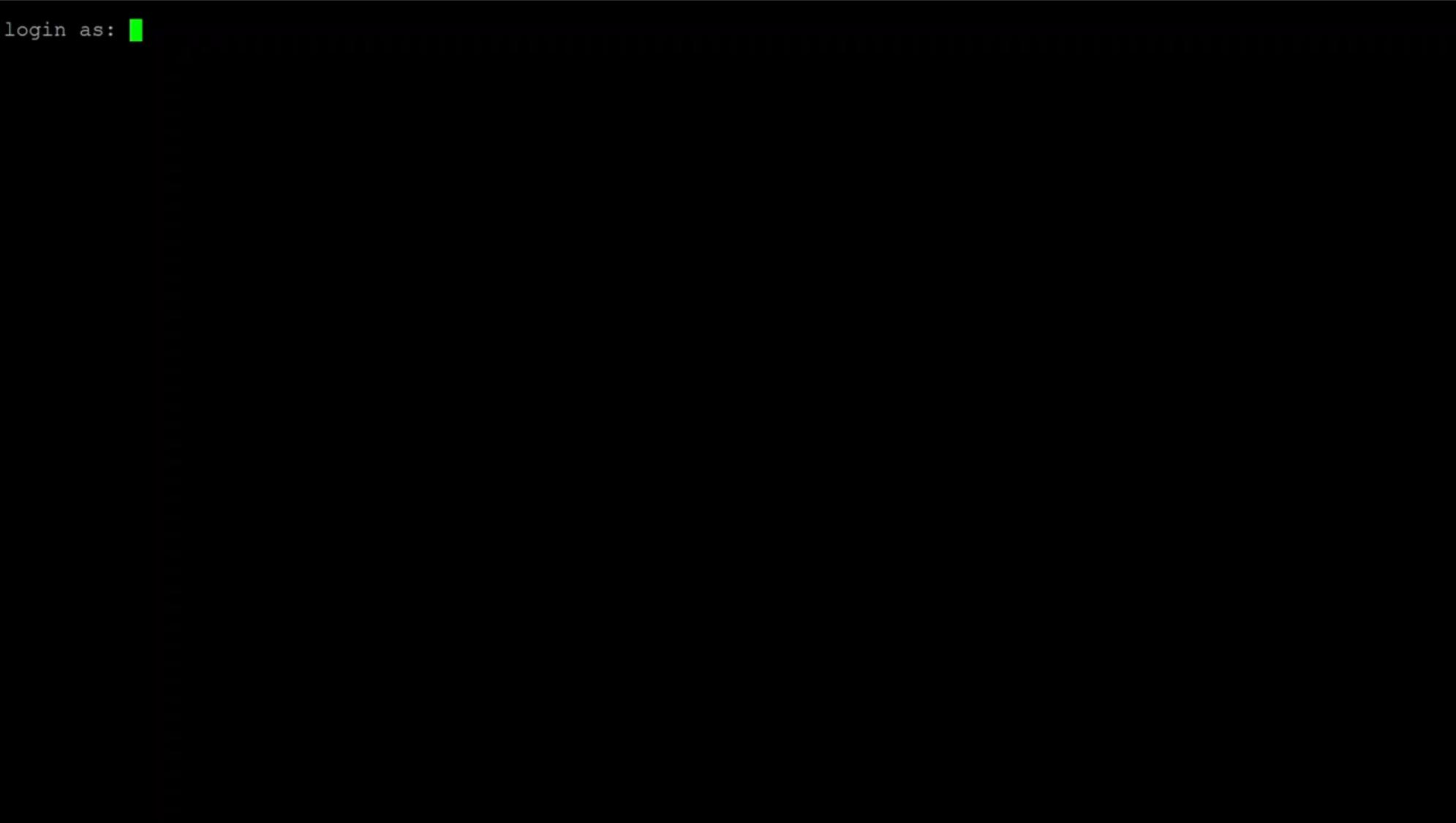
01 Product Overview



<https://youtu.be/ebN2kTGZIRE>

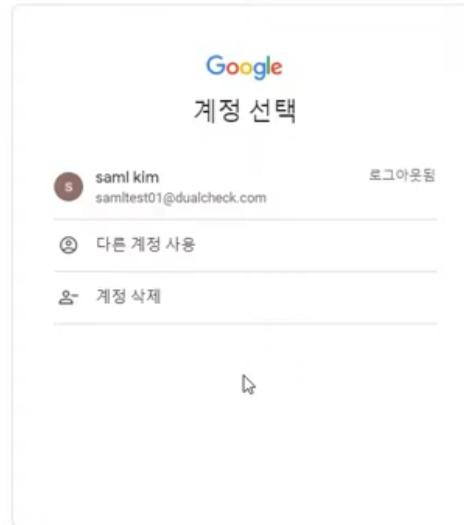
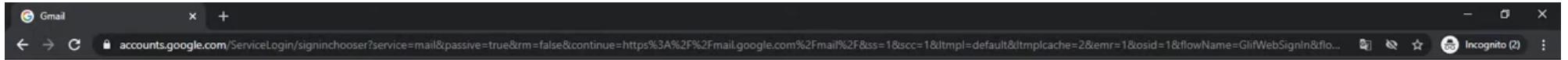


<https://youtu.be/cjmjBDwggw00>



<https://youtu.be/FDt0i06otUI>

01 Product Overview



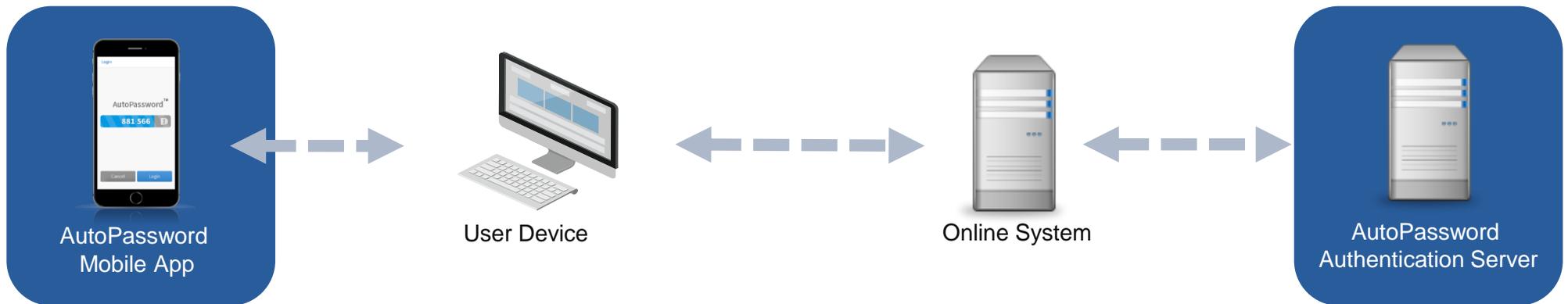
한국어 ▾ 도움말 개인정보 보호 약관

<https://youtu.be/I5H1C9gz7tg>

AutoPassword Architecture

To switch to AutoPassword, you only need to add the AutoPassword authentication server and the AutoPassword mobile app to the existing online system. This allows you to build a secure and convenient authentication environment without significantly changing the existing service structure. The administrator first installs the AutoPassword authentication server, and then integrates the AutoPassword API to enable communication between the online system and the authentication server. API integration is the setting that allows the AutoPassword to be displayed in the service.

The user must install the AutoPassword mobile app from the app store. After installation, the user goes through an identity verification process to link the user's account with the mobile app. In this process, the user's ID and app are registered with the authentication server, and afterward, the user can securely access the online system through AutoPassword verification and out-of-band biometric authentication on the registered smartphone.



01

Product Overview

02

Key Features

03

References

04

Contact

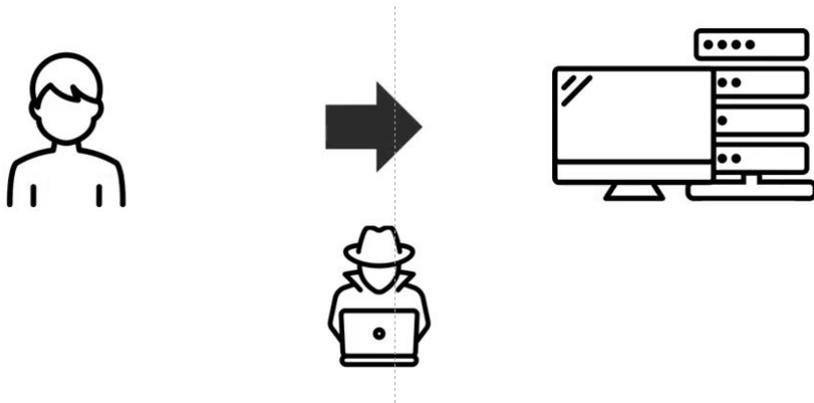
02 Key Features

Feature 1 – Authentication technology secure against phishing, pharming, and man-in-the-middle attacks

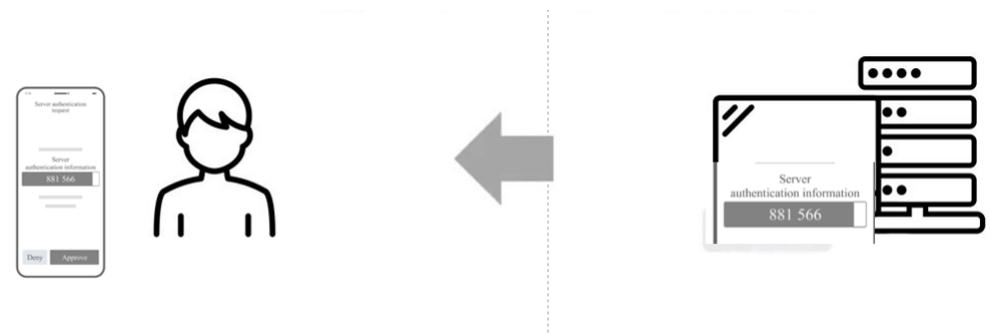
AutoPassword is not a method in which the user directly enters a password, but a method in which the online system generates and displays an AutoPassword, the user verifies it, and then the user authentication value is delivered to the online system through smartphone communication.

Thanks to this structure, neither passwords nor authentication values are entered or stored on the user's device during the authentication process, and as a result, attempts to steal authentication information that occurred in conventional methods, such as phishing, pharming, and man-in-the-middle attacks, are fundamentally neutralized.

Input-based authentication technology
vulnerable to theft or misuse



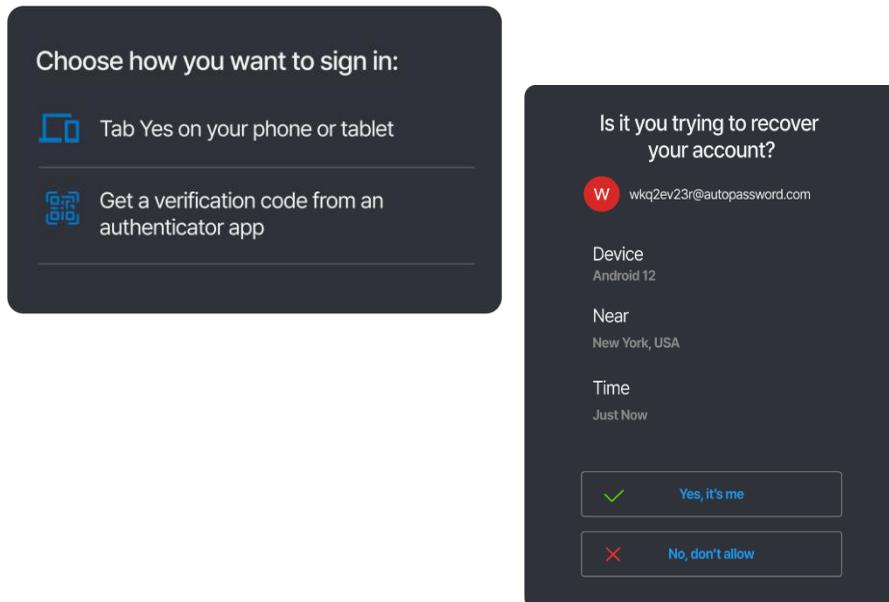
Output-based authentication technology
immune to theft or misuse



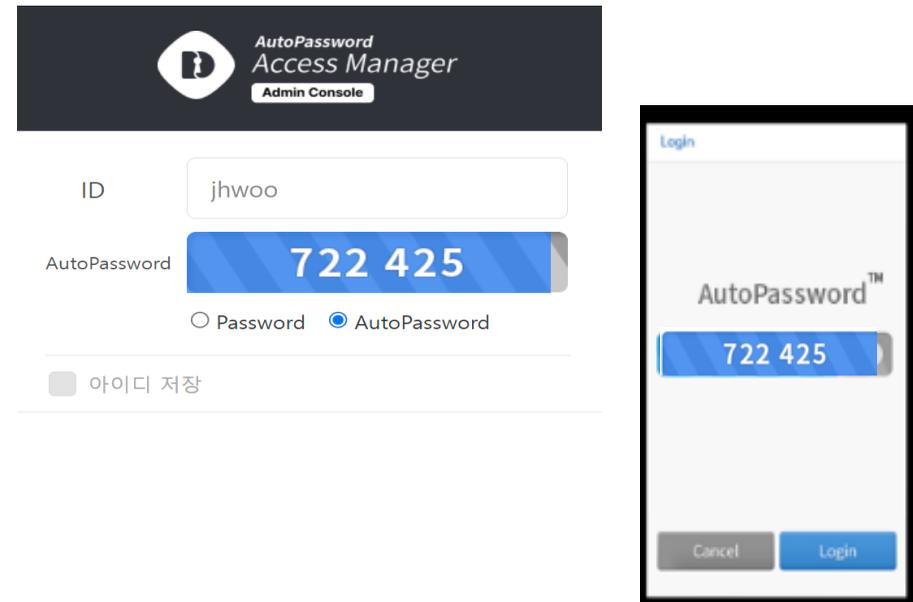
Feature 2 – Mobile Mutual Authentication Technology

Conventional mobile authentication technology is a user verification technology that sends a push notification or text message to the user's smartphone, and the user checks and approves it. The mobile user authentication method only verifies that the user possesses a "legitimate mobile authenticator," but it does not verify whether the service the user is accessing is an actual legitimate system. As a result, if the user is accessing a phishing site or a disguised system, the user may inadvertently approve the authentication request, leading to authentication being stolen. In contrast, AutoPassword is a mutual authentication technology that uses mobile devices but allows the user to first verify the system they are accessing.

Mobile authentication technology that authenticates only the user



Mobile mutual authentication technology that authenticates both the online system and the user simultaneously

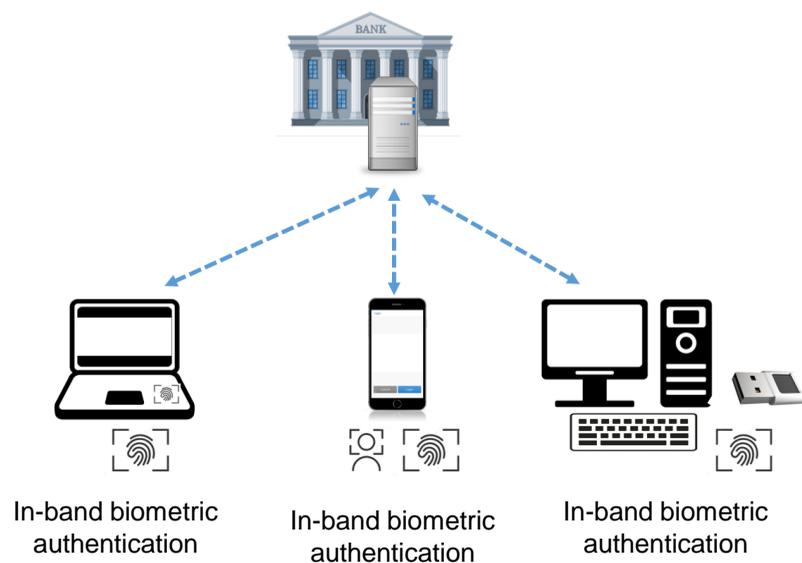


Feature 3 – The Most Economical Biometric Authentication Technology

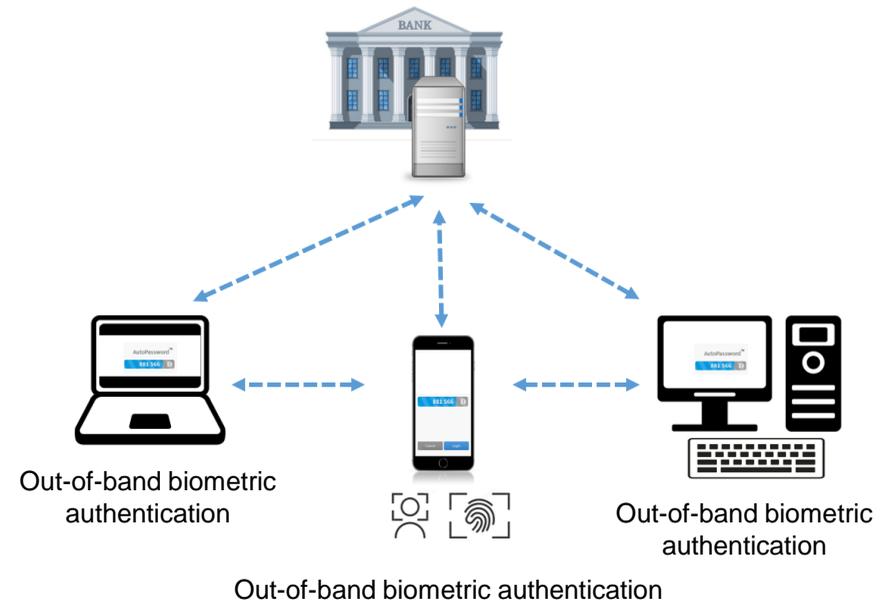
Conventional biometric authentication technologies such as FIDO or Passkey are “in-band biometric authentication” technologies, which require that each user device performing authentication must be equipped with a biometric sensor. While smartphones are generally equipped with fingerprint or facial recognition sensors, desktops and some laptops do not have such sensors, and therefore, to use biometric authentication in a PC environment, additional hardware sensors must be purchased and installed.

In contrast, AutoPassword adopts an “out-of-band biometric authentication” method, which allows users to utilize the biometric sensor already built into their smartphone to perform out-of-band biometric authentication on various devices such as desktops and laptops. The out-of-band biometric authentication method eliminates the need to add separate biometric sensors to PCs or laptops, drastically reducing the cost of device adoption.

In-band biometric authentication
that requires a biometric sensor on each device



Out-of-band biometric authentication
that does not require a biometric sensor on each device



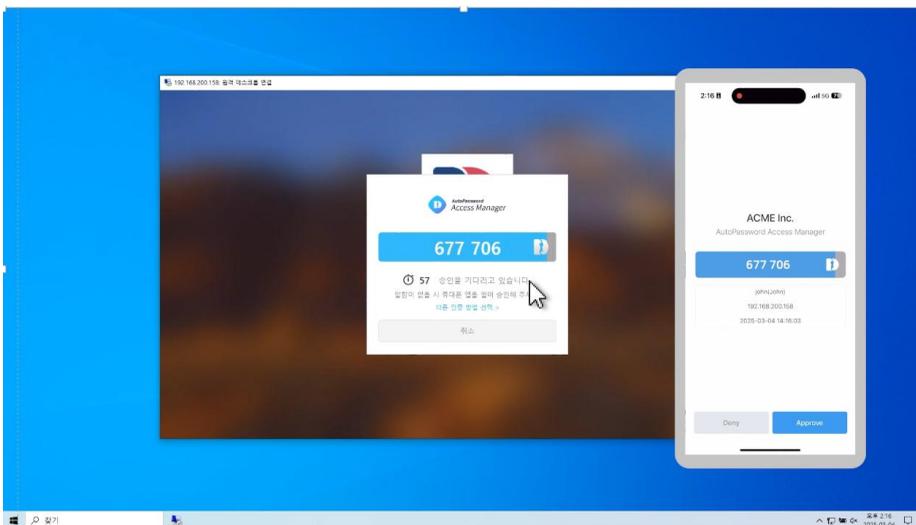
02 Key Features

Feature 4 – Biometric Authentication Technology Supporting Cloud and IoT Devices Where Sensors Cannot Be Added

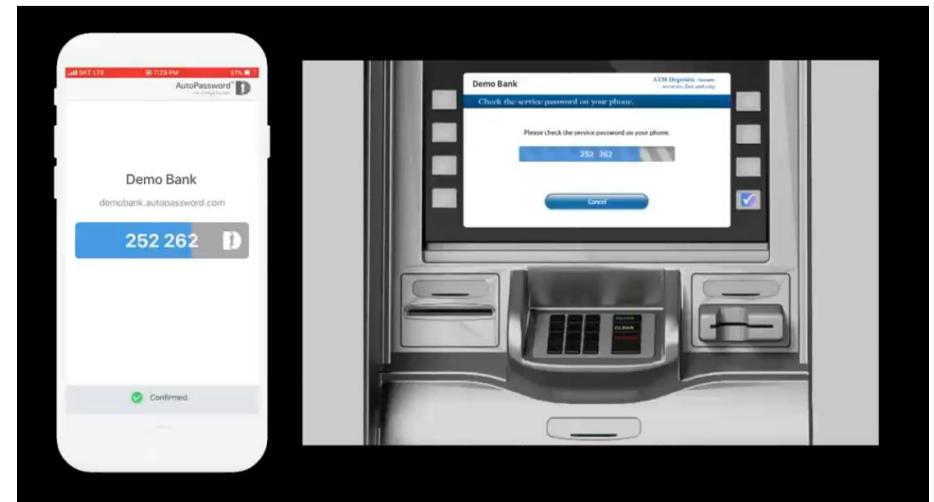
To apply biometric authentication in cloud or IoT environments, the device must be equipped with a biometric sensor. However, many cloud devices or IoT devices do not have USB ports or Bluetooth functions that allow biometric sensors to be added, and in such cases, passwords ultimately have to be used again.

AutoPassword resolves this limitation by using out-of-band biometric authentication technology. On a cloud or IoT device equipped with a screen, the AutoPassword is first presented, and the user approves it with the biometric sensor on their smartphone, enabling secure authentication even on such devices. Through this approach, the scope of biometric authentication can be extended beyond desktops and laptops to cloud and various IoT devices.

Remote cloud PC login using
out-of-band biometric authentication



ATM transaction approval using
out-of-band biometric authentication



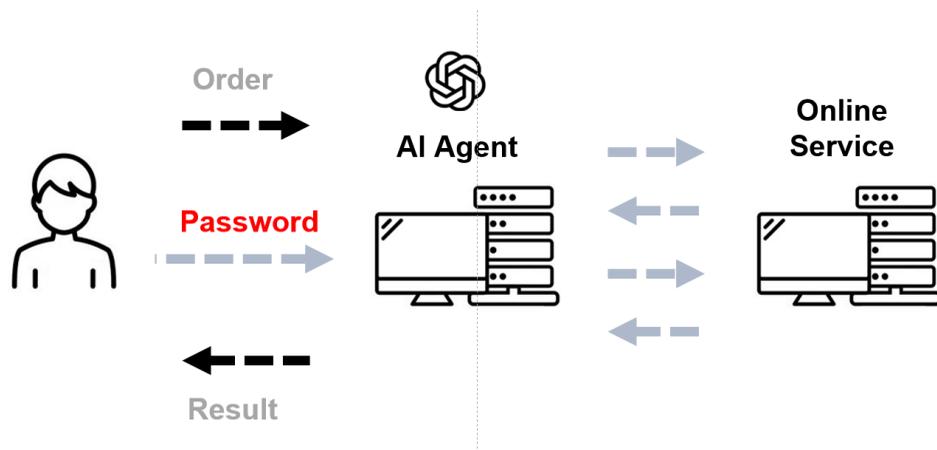
02 Key Features

Feature 5 – Out-of-Band Biometric Authentication Technology Extendable to AI Agents

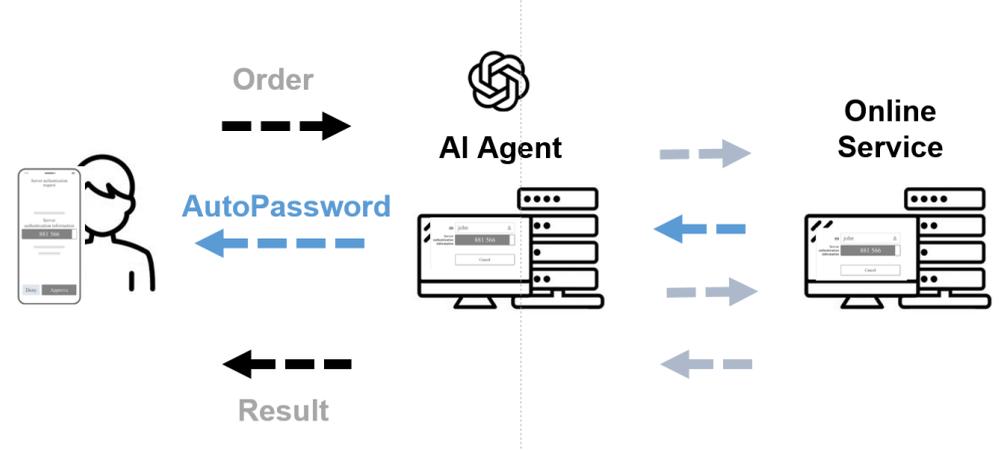
As the use of generative AI services, including ChatGPT, expands, it is important to verify whether the AI service being accessed is legitimate or a disguised service. AutoPassword allows the user to first verify the authenticity of the AI service before using it.

AutoPassword is also effectively used when utilizing AI agents. When using AI agents, there are situations where the agent must be provided with the user's password to perform tasks on behalf of the user. Providing passwords to AI agents poses a significant security risk. However, if AutoPassword is applied, the AI agent can present an AutoPassword to the user at the moment authentication is required during task execution, and the user approves it on their smartphone, eliminating the risk of password sharing. With AutoPassword, users do not need to enter passwords into AI agents. When authentication is required, the AI agent presents the AutoPassword to the user, and the user approves it, enabling safe use of AI agents.

Method in which the user enters a password into the AI agent



Method in which the AI agent presents an AutoPassword to the user



01

Product Overview

02

Key Features

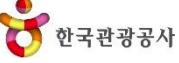
03

References

04

Contact

03 References

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

Awards



The Korea Internet Awards

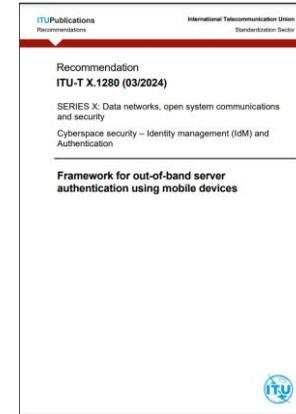


The Commissioner's Award

Standard Technologies



[TTAK.KO-12.0383](#)



[ITU X.1280](#)

Presentations



NEW YORK
FinovateFall 2016
Presenter

<https://youtu.be/w2NtbPVaHSK>



<https://youtu.be/rBUK45fdBtY?t=838>



NEW YORK
FinovateFall 2018
Presenter

<https://youtu.be/-DG-LYmRVfk>



<https://youtu.be/nF72E24BCec>

Certificates



ISO/IEC 25023, 25051, 25041



01

Product Overview

02

Key Features

03

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.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



- 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



Thank you