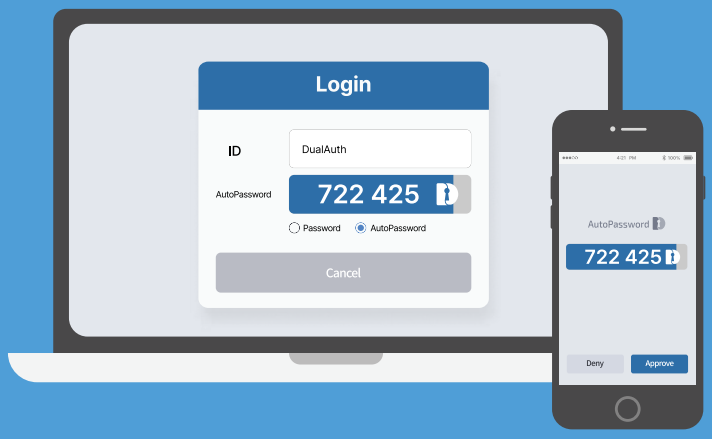
Korea Gov. Innovative Product | TTA GS Certified Level1 | New Excellent Product Certifed | Common Criteria Certified

IBM Security

Passwordless Solution for Zero Trust

Upgrade from weak passwords to the secure and convenient AutoPassword.

AutoPassword



AutoPassword, standardized as ITU-T X.1280, is a passwordless mutual-authentication technology. Instead of users entering passwords, the system generates a one-time AutoPassword and the user simply approves it with facial or fingerprint recognition. It removes the need to remember passwords and provides strong protection against phishing, pharming, and man-in-the-middle attacks.

AutoPassword is the most cost-effective out-of-band biometric authentication technology!

Existing biometric technologies such as FIDO and Passkey rely on in-band authentication, requiring a biometric sensor on every device—PCs, laptops, servers, and kiosks. This increases cost and forces users to register their biometrics repeatedly. When a user relies on a smartphone's biometric sensor on a device without its own sensor, they cannot confirm which online system is receiving their biometric data, creating a security vulnerability.

In contrast, AutoPassword enables secure smartphone-embedded biometric authentication even on devices without sensors. The online system first submits an AutoPassword, allowing the user to verify and approve it before providing their biometric authentication. (ITU-T X.1280)

In-band biometric authentication VS **Out-of-band biometric authentication**



Fingerprint Sensor Addition



Vein sensor addition



Smartphone-embedded biometric sensor

How AutoPassword works

The system submits the AutoPassword, and the user approves it



- When the online system submits an AutoPassword, the user verifies it in the smartphone app.
- When the user approves the AutoPassword, the user is authenticated via the smartphone's biometric sensor.
- International standard technology for mutual authentication between the user and the online system (ITU X.1280).

Existing Authentication vs. AutoPassword

Existing methods—OTP, digital certificates, mobile authenticators, and biometrics—authenticate only the user, leaving accounts vulnerable to takeover and shifting responsibility to the user. They also require high implementation costs. In contrast, AutoPassword provides mutual authentication between the user and the online system, delivering stronger security, lower cost, and greater convenience.

Biometric Authentication (FIDO, Passkey)

- High-cost structure requiring biometric sensors on every device (in-band biometric authentication).
- Security vulnerability when using smartphone biometrics on other devices—users cannot verify where they submit their authentication information.

Mobile Authenticator (Push or QR)

- If a fake system sends a push message, the user cannot verify the requester, leading to authentication theft.
- If a fake QR code is scanned by a smartphone and approved, user authentication is stolen.

Certificate

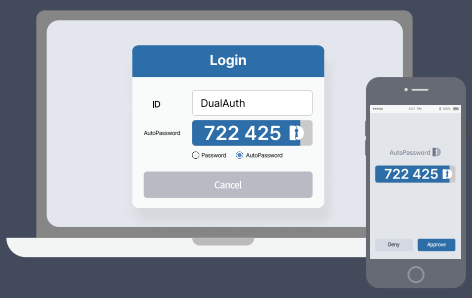
- Risk of NPKI folder and certificate file theft
- Difficulty managing user private keys

One-Time Password (OTP/SMS)

- Cannot verify service authenticity when connecting to a fake online system
- OTP codes can be stolen or phishing

VS

AutoPassword



- The convenience of the system submitting an AutoPassword for user approval
- The security of mutual authentication that verifies the legitimacy of both the online system and the user
- The cost-effectiveness of using smartphone biometric authentication out-of-band, even on devices without biometric sensors

Major Clients KB국민은행 우리은행 유안타증권 KIAT 한국관광공사 KOMSA 한국해양교통안전공단

Implementation and Partnership Inquiries

www.dualauth.com +82-2-6925-1305 sales@dualauth.com