AutoPassword™

WHITE PAPER

AutoOTP & AutoPassword

Out-of-band mutual authentication system combining biometric authentication and server authentication

Prepared By:
John Woo, CEO
+82-10-3386-4017
jhwoo@dualauth.com

Table of Contents

Executive Summary

The authentication method is the most fundamental technology to provide personalized online services. A personalized online service is possible only when the user attempting to log in can be identified and verified whether it is a previously registered user.

Passwords, which are traditional user authentication methods, are being replaced by PKI certificate technology, FIDO biometric authentication technology, and mobile push authentication technology. However, it still has the inconvenience of having to re-register the authentication method every time the terminal is changed, or the limitation of exposure to attacks impersonating service providers has not been solved.

This document explains the limitations of existing authentication technologies and presents AutoOTP and AutoPassword, which combine out-of-band server authentication and biometric authentication, to explain how the out-of-band mutual authentication technology works independently of the terminal and against man-in-the-middle attacks.
Lastly, it explains how the new out-of-band mutual authentication technology improves security and convenience in government agencies, banks, corporations, and institutions.
This document is written for corporate security officers or online service administrators who need to select an authentication method.

The advent of various user authentication technologies and how to distinguish authentication technologies

User authentication technology continues to evolve based on security and convenience. Starting with user password, security card (code table), one-time password dongle, one-time password service through SMS/ARS/e-mail, PKI certificate(X.509), user authentication technology is advancing through FIDO-based biometric authentication such as fingerprint/iris/face recognition, and block chain-based DID authentication.

Security card, PKI certificate, fingerprint/iris/facial recognition, block chain DID authentication technology examples

As a way to understand the various authentication technologies that are being advanced, there is a method to analyze how individual authentication technologies operate, but it can also be quickly understood through the classification method that classifies authentication technologies in a technology standardization organization. There are three main ways in which standardization organizations classify authentication technologies :
classifying by factors, classifying by communication method, and classifying by security level.

The method of classification by factor is a classification method of what factors can authenticate the user in identifying the user. The classification through the communication method is a classification method by the communication channel that delivers the authentication value. Finally, the classification by security level is a method of classifying which authentication method is the more secure authentication method.

Classification by Factor

Classification by factor	**Explanation**	**Example**
Something you know	Method proven by what the user knows	Memorized password or PIN
Something you have	Method proven by what the user possess OTP dongle, USIM-based mobile authenticator, etc. (However, the method of providing the authentication code by text message, ARS, e-mail, etc. is a service subscription method rather than possession, and it is not possible to prove possession in the case of an attack such as call forwarding, so it is excluded from possession-based authentication methods.) Can be used in combination with other factors to activate the proof of possession authenticator (something you know or possess)	security card (password), Out-of-band authenticator (a mobile authentication app that transmits push-based authentication code or scans a QR code or a mobile authentication app that confirms possession of a USIM), single factor OTP generator, Multi-factor OTP generator (fingerprint recognition/PIN input OTP), single factor encryption software (file-based certificate), Single-factor encryption device (security token for storing certificates, button-type authentication device connected to the terminal), Multi-factor encryption software (file-based certificate combined with biometric authentication in mobile devices, FIDO), Multi-factor encryption device (file-based certificate combined with biometric authentication in a dedicated authentication device)
Something you are	Method proving with the user's biometric information Since biometric information itself is not secret and operates based on probability, it is recommended as a factor supporting other definitive authentication methods in consideration of the false acceptance level. Rather than the service provider's centralized biometric authentication value comparison method, it is recommended to store and compare biometric authentication values in the user's own terminal.	used as an additional factor of something you possess

Classification of Authentication Technology by Communication Method

Operation Method	Explanation	Example
In-band authentication technology	A method of transmitting user authentication values through a communication channel between the user terminal and the service server	1. A method of entering user password/security card/one-time password (OTP dongle/SMS/ARS/Email, etc.) in the user PC connected to the online service 2.A method of authenticating a user with an X.509-based certificate on a user PC connected to an online service (PKI certificate) 3. A method of verifying a user using a facial or fingerprint sensor on the user's phone connected to the online service and delivering the user authentication value to the server (FIDO)
Out-of-band authentication technology	A method of transferring the user's authentication value through a communication channel other than the communication channel between the user terminal and the service server	1. Method to receive push-based authentication request and approve it on mobile 2. Method of directly entering or scanning the authentication code or QR code displayed on the PC screen into the mobile app 3. Method of entering the one-time code displayed on the PC screen into the ARS phone

Classification by security level - AAL(Authentication Assurance Level)

Assurance Level	**Explanation**	**Example**
Level 1	Technology that identifies a user with one or more factors known only to the user, possessed by the user, or biometric factors that can identify the user	Receiving the input of the memorized user password
Level 2	Technology that identifies users with two or more factors out of three factors, and is resistant to reuse attacks using stolen code	A method of receiving the memorized user password and the one-time password generated by the OTP generator one has, Certificate that can be installed and uninstalled on PC or mobile with user password and software type
Level 3	A technology that uses encryption protocols such as SSL/TLS to not only confirm that the user has the encryption key, but also to confirm that the connected service is the correct service (Resistance to fake online services that are impersonated and the ability to prepare for attacking verification servers, etc.)	A method to prepare for not only user authentication but also online service attacks impersonating services by using the user certificate stored in the physical security medium (security token) and the server certificate that can verify the service, FIDO (UAF/CTAP2)

Limitations of User Authentication Technology

If we compare the latest authentication technology trends with the three authentication technology classification methods, the classification by factor is spreading as biometric authentication technology is recommended as an auxiliary means of authentication factors, combined with smartphones, which are possessed factors. As for the communication method, as the number of smart devices of users increases, the terminal-independent external authentication method is preferred from the terminal-dependent in-band authentication method, and the method classified by the security level is used to authenticate not only the user but also the service. In other words, it is a mobile authenticator using biometric authentication technology, supports out-of-band authentication that can be used in multiple terminals, and is evolving into a method that can check not only users but also service providers.

However, since mobile biometric authentication technology (FIDO) is an in-band mobile authentication technology, user authentication is effective only for applications running in mobile. For example, when user authentication is required in an application running on another PC or tablet, the biometric authenticator of the smartphone cannot be used as an authentication means. (Ex. It cannot be used as an out-of-band authentication method to authenticate the Internet banking user of the PC with the biometric authentication technology of the smartphone when user authentication is required in a situation where Internet banking is used on the PC..)

If the mobile authentication technology, which is an in-band authentication technology, is used out of band forcibly, it can be ineffective against an attack impersonating a service provider. As shown in the figure below, if a user authentication request is initiated out of band after the service provider that the user accessed connects to an attacker who pretends to be a service provider rather than a real service provider, the user may make a mistake by considering the authentication request was generated by his/her own connection. and approve the attacker's authentication request. If the in-band authentication technology is operated out of band, it becomes vulnerable to attacks impersonating the service provider.

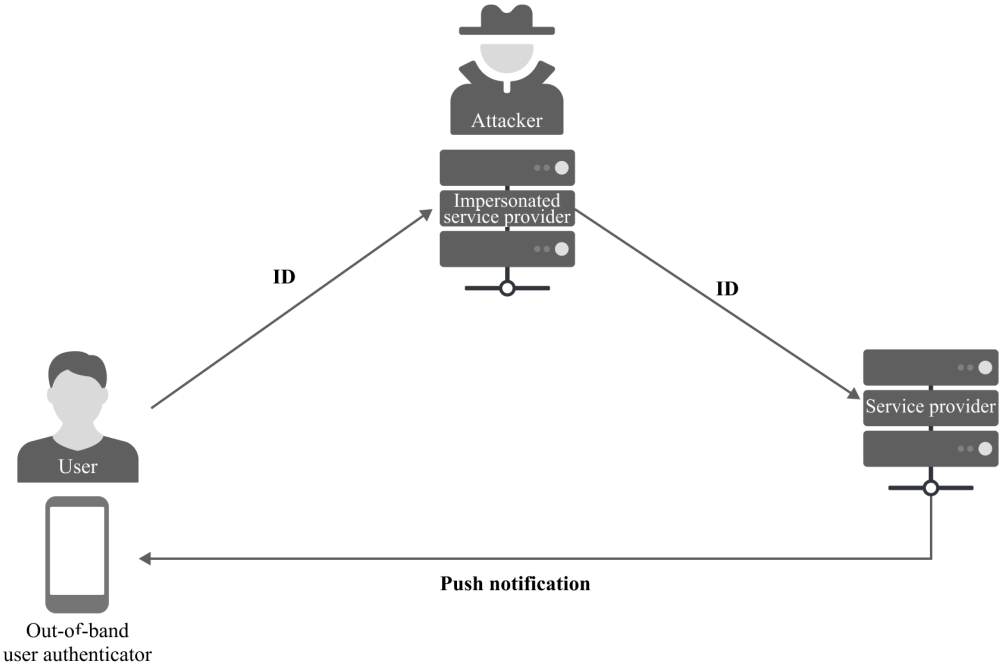


Diagram 1 : Vulnerability that occurs when in-band authentication technology is used out of band

In addition, since biometric authentication technology is an in-band authentication technology, in order to be used in multiple user terminals, the complexity of having to register one's own biometric information for every terminal equipped with a biometric sensor occurs.

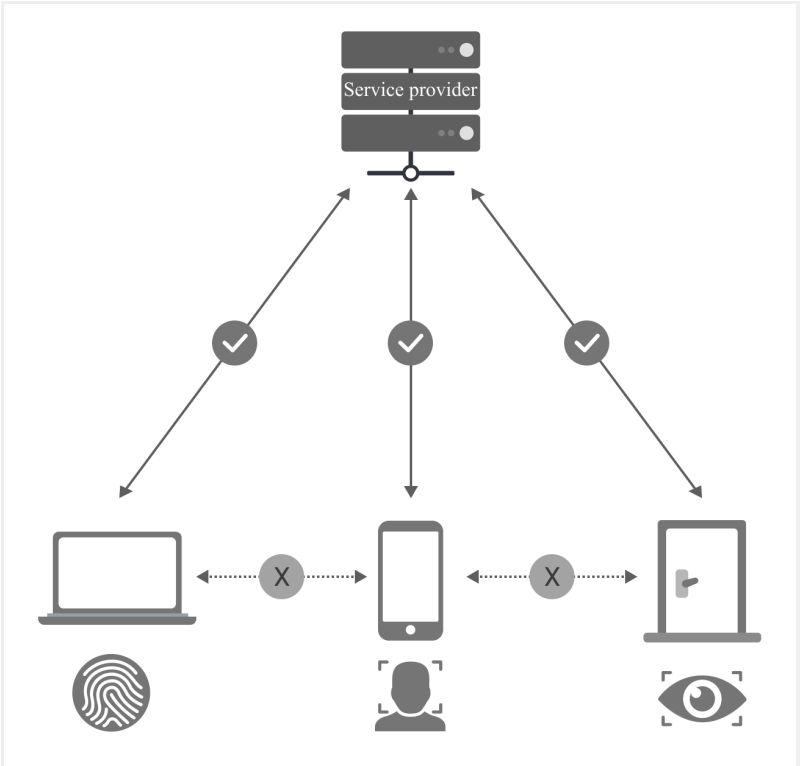


Diagram 2: In-band biometric authentication requires re-registration for each terminal.

In order to avoid the inconvenience of the terminal-dependent authentication technology possessed by the in-band authentication technology, attempts have been made on an external independent authenticator that is connected to the terminal device through Bluetooth or USB communication, but since wireless and wired connection methods are different for each terminal device to which the authenticator is connected, a single external authenticator cannot support connection methods with all terminals. For example, when an external authenticator is connected to a PC by wire, it must have a physical port (USB A, B, C type) interface supported by the PC. There is no external authenticator that supports all these communication methods.

An external authenticator tried a mobile-based FIDO CTAP2 authentication method using Bluetooth of a smartphone and a PC in order to escape the compatibility of the physical medium with the terminal, it is difficult to develop a smartphone-based Bluetooth CTAP2 authenticator that can cover all applications and hardware types because it is possible to match the PC Bluetooth version, operating system version, application version, and Bluetooth pairing and communication protocol for each smartphone type. For example, in the case of Google, after registering an Android phone to a PC through Bluetooth, only a limited authentication service is provided to allow Android CTAP2 authentication only in Google services through the Google Chrome browser.

Therefore, there is a need for a new authentication technology that includes the user's biometric authentication and can operate as a terminal-independent external authenticator and has security that can verify even the service provider.

AutoOTP and AutoPassword Combining Out-of-Band Server Authentication Technology and Mobile Biometric Authentication Technology

In-band Server Authentication Technology and Limitations

A common way to prepare for attacks impersonating service providers is to check the SSL/TLS server certificate. The SSL/TLS server certificate can be checked through the green bar and lock of all web browsers according to the X.509 standard. Server certificate is a typical in-band server authentication technology, since it is a technology that can only be verified through a web browser connected to the

.

However, since the web server certificate technology is separated from the user authentication methods, the user has the inconvenience of having to separately check the server certificate each time the user accesses the web service, which is easily overlooked by the user. In addition, if you encounter an attacker who provides a server certificate using a similar domain, you can easily steal the user authentication value even if there is a lock on the green bar. In addition, the SSL/TLS server certificate works only in the web browser that manages the public key of the certificate issuer, so there is a limitation that it cannot be used in an installed application or operating system other than a web browser. Rather than being used as a server authentication technology, the web server certificate is mainly used as a communication channel encryption technology.

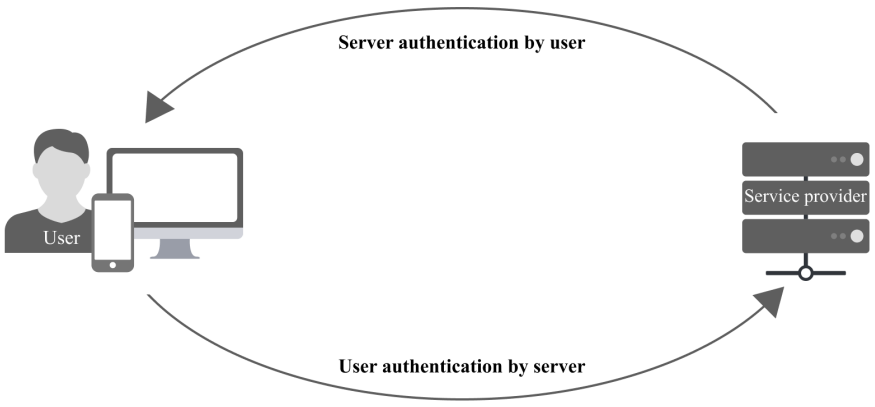
Out-of-Band Server Authentication Technology

To overcome the limitations of in-band server authentication technology, ITU-T SG17 is in the process of standardizing out-of-band server authentication technology (X.oobsa). The out-of-band server authentication technology is a technology that simultaneously authenticates the server and the user with the user's mobile authenticator. In out-of-band server authentication technology, the server connected to the user's PC terminal first presents a one-time password for server verification on the user's screen, and the user

authenticates the server by checking whether it matches the one-time password for server verification generated by the server authentication app installed on the smartphone. If the one-time password presented by the server matches the one-time password generated by the server authentication app installed on the user's smartphone, the user authenticates that the connected server is a verified server.

User Authentication Technology Combined with Out-of-Band Server Authentication Technology

When the user verifies the one-time password for server verification on the smartphone, the smartphone app checks the user's biometric authentication value and provides the user's authentication value to the server if it is a legitimate user. As for the user authentication technology used at this time, verified traditional user authentication technologies such as OTP, PKI, and FIDO combined with biometric authentication are applied.

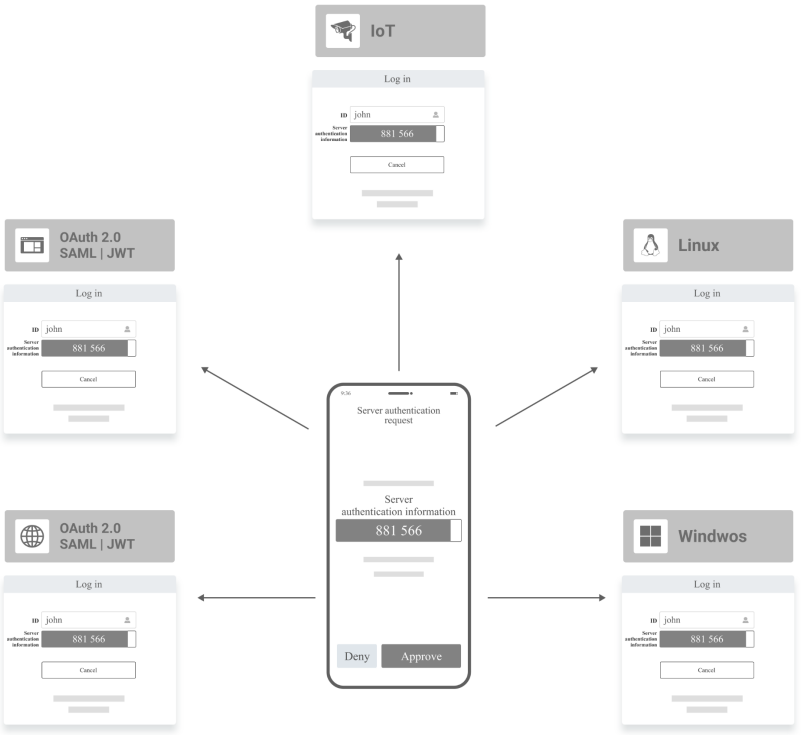


Technical Effect

1. **User-centered mutual authentication technology that performs server authentication and user authentication at the same time**

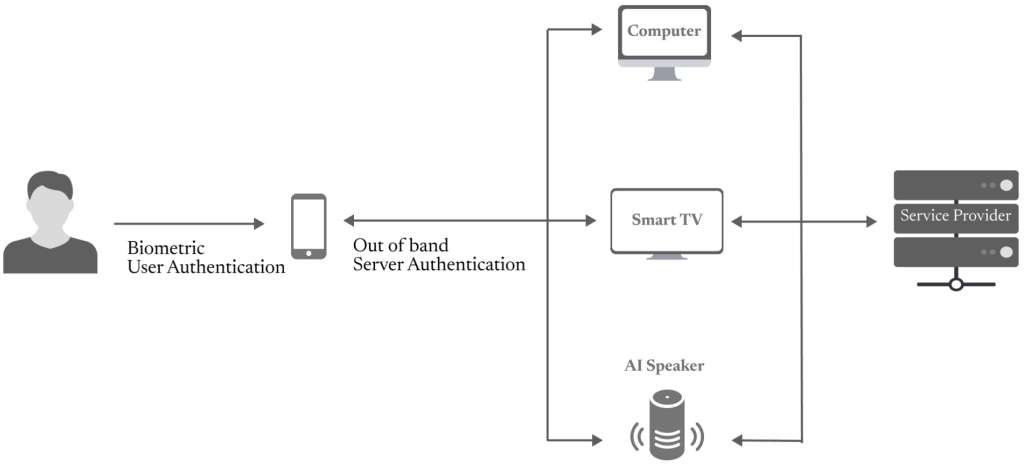
SSL/TLS server certificate, an in-band server authentication technology, is separated from the user authentication process, so unless the user intentionally checks the server certificate, only the user authentication proceeds without the server authentication process.

Using this user behavior pattern, an attacker steals user authentication information by inducing users to a pharming site with the same domain name or by inducing access to a malicious site with a similar domain name displaying a lock. However, this is an out-of-band mutual authentication technology that combines out-of-band server authentication technology and user biometric authentication technology. The server first presents an explicit one-time password for server authentication to the user. The app provides the user's authentication information to the server, and the server also verifies the user. That is, out-of-band mutual authentication was made by linking the server authentication process and the user authentication process.



2. Expanding mobile biometric authentication technology to user terminals that do not support biometric authentication

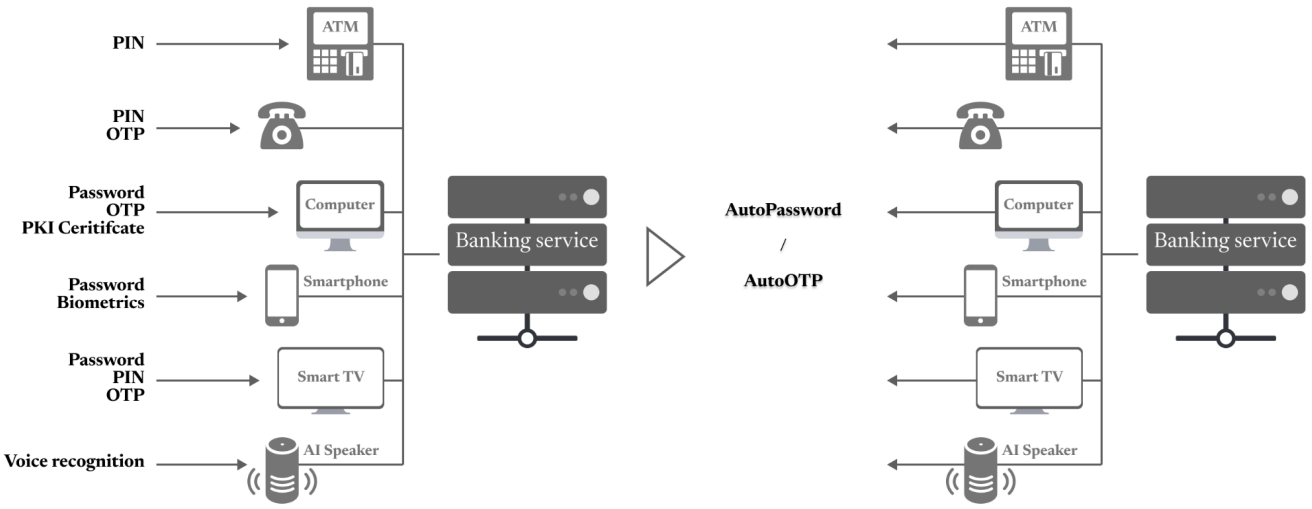
It provides an out-of-band mutual authentication technology that enables the biometric authentication technology, which was only valid in terminals equipped with a biometric sensor, to be applied to a terminal not equipped with a biometric sensor. By using the out-of-band mutual authentication technology, the vulnerability to the service provider impersonation attack possessed by the out-of-band user authentication technology can be resolved, and the user biometric authentication technology locked in the smartphone can be extended to terminals without a biometric authentication sensor. For example, a user can perform user authentication of a PC by using facial recognition or fingerprint recognition in a smartphone on a PC without a biometric sensor such as a fingerprint reader or camera. That is, the out-of-band mutual authentication technology can confirm where the user submits the biometric authentication value, so it is safe to use the out-of-band biometric authentication technology.



3. Mutual authentication technology that can integrate fragmented user authentication methods for each terminal into one

At an ATM, you must present your card and PIN code; in telebanking, you must enter the OTP code; in Internet banking, you must enter PKI certificate and OTP; and in mobile you must present your fingerprint or face. In smart TVs, OTP must be entered with the remote control; and in AI speakers, after registration of voice, authentication must be performed. This is because the terminal-dependent authentication method is used, in which the authentication method is different for each service channel.

However, when AutoPassword, an out-of-band mutual authentication technology, is applied, one authentication method can be applied to all service channels. Since all service channels provide service authentication information to the user first, and the user approves it, a unified authentication method can be used even if each channel is different.



4. Manage user passwords together

Whenever the user authenticates the one-time password provided by the service on the mobile device, the user password of the service is automatically updated, freeing the user from the password management in which the user has to change and memorize the password. Out-of-band mutual authentication technology is a means of replacing user passwords, but does not eliminate user passwords. Even if all authentication technologies shout "Kill Password" or "Passwordless", there is still a limit to restore the user's password in case the smartphone is eventually lost. This out-of-band mutual authentication technology does not require the user to change and manage the password because the user's password is updated randomly by mixing upper and lower case letters, special characters, and numbers every time the user authenticates the service provider- thus if a user loses or renews a smartphone, he or she can log in to the online service and use it after going through the identity verification process and resetting the user's password. Also, when the user changes the smartphone, it is possible to reset the out-of-band mutual authentication app.

AutoOTP and AutoPassword Use Cases

1. **Banks and government agencies that conduct business with PCs**

20,000 executives and employees installed the AutoPassword app on the user's smartphone without purchasing a separate biometric sensor in the PC to perform their work through PC, thereby automating log-in to workplace PCs and web services. Whenever a user attempts to log in, an automatic password is presented to the user and the user verifies it with the AutoPassword mobile app, thereby freeing the user from password management and greatly improving security. In particular, it freed users from the administrative burden of changing user passwords every 3 months and having to memorize them, and with the voluntary introduction of users, change management for security has been greatly improved.

2. **Online store offering high-priced point services**

AutoOTP was applied to prevent account theft in online stores that provide online wholesale services and provide retailers with points that can be used like cash. In contrast to the previous general OTP, the user had to read and enter a 6-digit code, the wholesale online store solves the inconvenience of entering the OTP code by presenting the AutoOTP code first and the user checking it on the mobile app, and provides security that cannot be hijacked.

3. **Gmail service for enterprise and cloud service**

In companies where important work is done through Gmail, the user authentication method was replaced with AutoPassword to prevent the user's email account from being hijacked from phishing or pharming attacks. When using cloud services through a home or office PC, tablet, or smartphone, a separate biometric registration process was required for each device, but it is now possible to skip the registration process of user authentication means for each device by verifying it on a smartphone.

4. **Access control of critical servers**

When an administrator accesses a service server that stores and operates important data, the key file input method or OTP code input can be easily hijacked through the administrator PC. If malware penetrates the administrator PC, all account data and input values in the administrator PC can be hijacked by a third party. By introducing AutoPassword, instead of the user entering the authentication value when accessing

the Linux server, the Linux server presents the authentication value to the user and the user verifies it with a smartphone out of band, so access control of the server can be implemented safely.