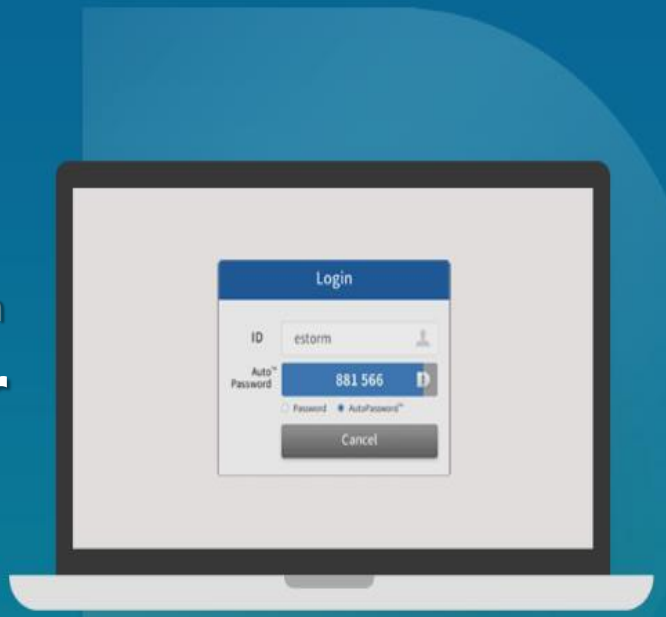
Safe and Convenience PC & Server Access Management System

AutoPassword Access Manager

Product Information



DualAuth

AutoPassword
Access Manager

"Safe and Convenience PC & Server Access Management System"

AutoPassword Access Manager

1. Problems of Password Management

The reality of difficult password management

Even though the security protocol that doesn't allow users to use work PCs at will exist, someone can still shoulder-surf as users enter their passwords, and there could be a situation where PC passwords are shared among co-workers under inevitable circumstances. Also, since, in reality, it is difficult to memorize passwords even though it is required to change the password, following a specific cycle, users tend to use values that are easy to remember or write them down on their desks. It is hard to prove who is to blame when there is a security incident taking place on a specific PC.

Shoulder Surfing or Phishing ID/Password

ID/Password sharing of PCs and Servers

Impossible to prove the intentionality after the incident

Frequent password changes and difficulty in remembering

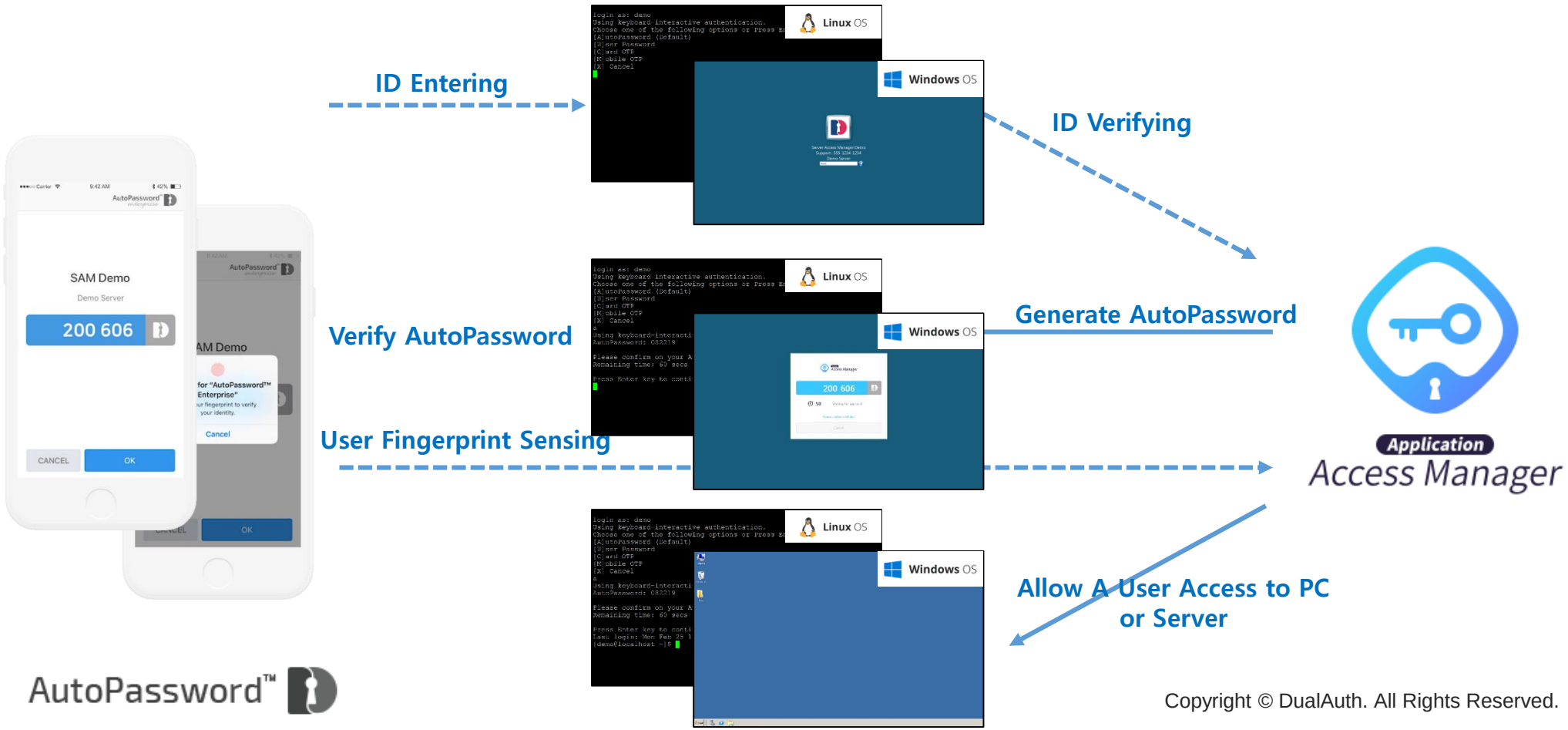
Carrying a complex and inconvenient 2FA device

Increase in management manpower costs due to the loss of passwords

AutoPassword™

AutoPassword-based PC and Server Access Management

AutoPassword Access Manager is a mobile-based PC and server access management solution which makes users no longer need to change or memorize the password since the PC or Server provides the AutoPassword™ by itself and the users verify it on their mobiles, not the users entering their passwords. Instead of the user password, it uses AutoPassword, so it gives the security without credential breaches and the convenience with automatic user password updating in OS. It makes the user free from password management.

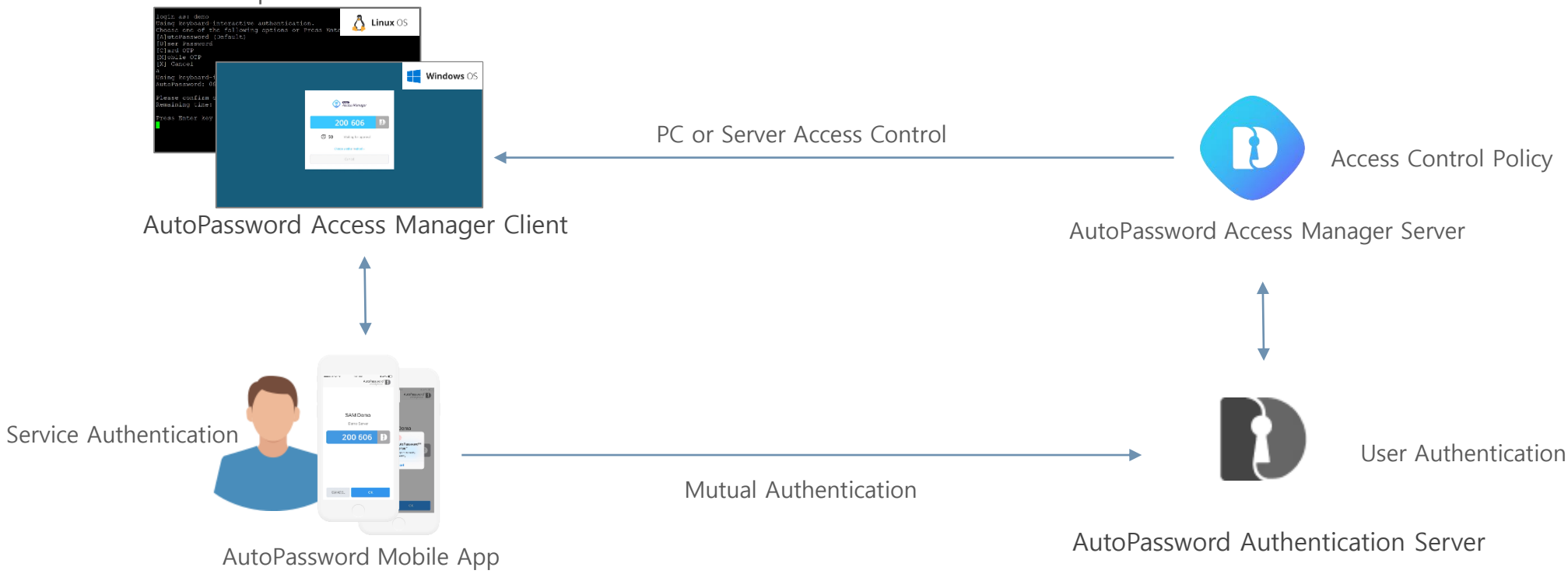


AutoPassword™

3. AutoPassword Access Manager Structure

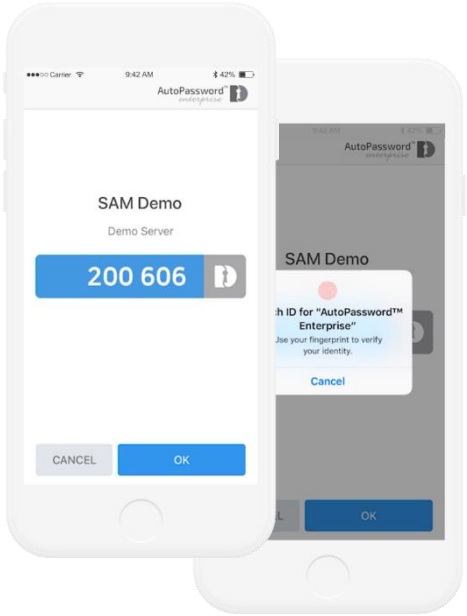
Access Control Client and Server connected with AutoPassword

AutoPassword Access Manager consists of the Access Manager client program that manages the operating system ID and password installed on the user's PC or Server and the Access Manager server that can set up the user ID and the usable PC and Server. After the admin installs the client program on the designated PC or Server and designates the user within the AutoPassword Access Manager server, only the designated user can use the corresponding PC or Server. When the mutual authentication technology, AutoPassword, is connected to Access Manager, the user can log on to the PC or Server, using his or her smartphone.



4-1 Logon after mutual authentication between the user and the PC or Server

Users no longer need to change or memorize the PC or Server password since the PC or Server provides the AutoPassword™ by itself and the users verify it on their mobiles, not the users entering their passwords. Also, the PCs or Servers allow the users to use their PCs or Server after verifying the users' phones and the users biometrics. (Smartphone's biometric authentication is a default installation/FIDO is an additional option)

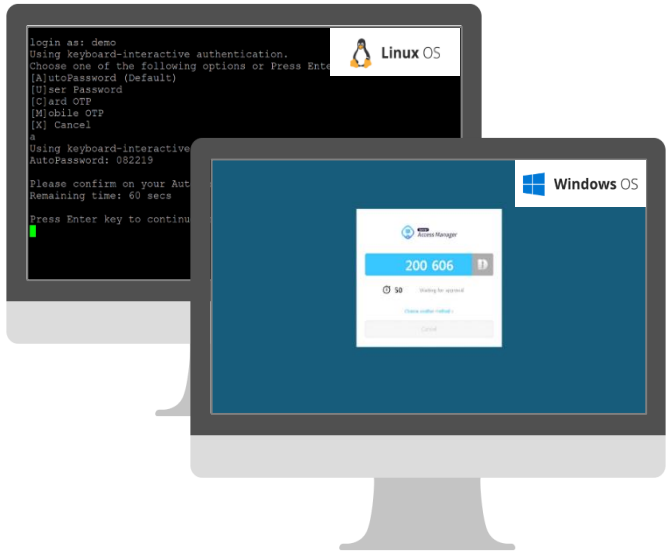


PC Confirms

One time password technology

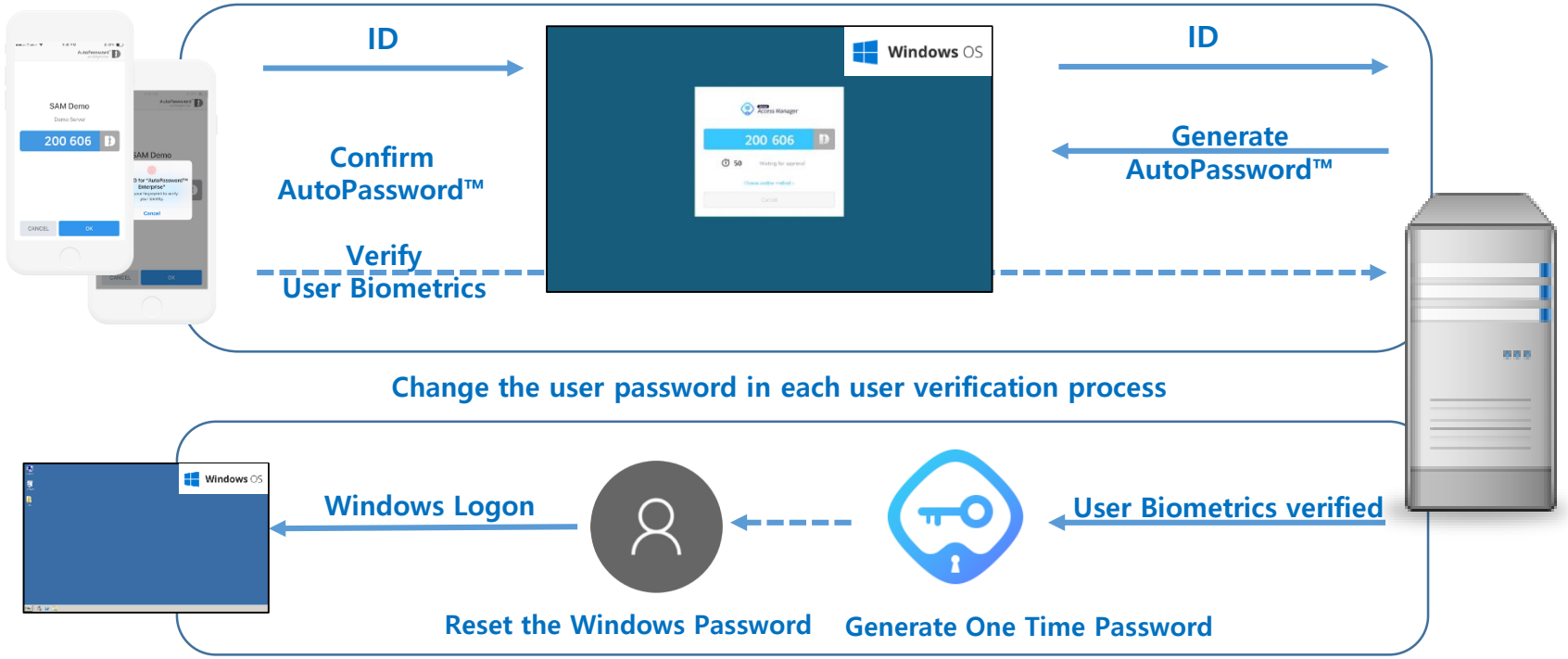
User Confirms

Biometric authentication technology



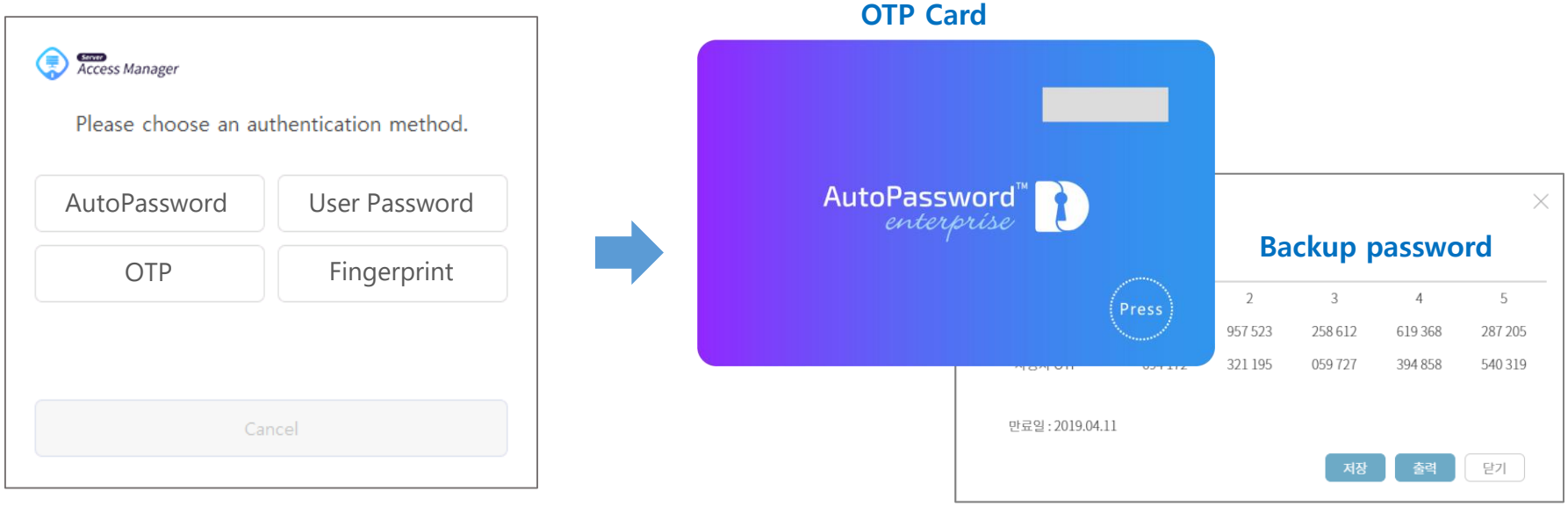
4-2 Automatic changes of OS passwords in each user verification process

If a user install AutoPassword Access Manager client on their PC or server, the user password of OS automatically changes during the process of users verifying one time AutoPassword™ provided by the PC or Server. The user password that the PC or Server uses internally is set as a randomly generated complex value, and the user just needs to confirm whether it is the same AutoPassword™ generated on the user's smartphone without the need for users to memorize or change the user password.



4-3 Alternative logon method in case of losing a smartphone or a network of PC

AutoPassword Access Manager can provide a backup password printed on a piece of paper or through an email for the users to be able to use their PCs by the admin in case of loss or destruction of a smartphone, and can change the password type for them to log on to PCs and servers using their user passwords instead of AutoPassword™. Also, AutoPassword Access Manager provides the OTP-based logon service for users to be able to use their PCs in a situation where no network is available when they are on the move or having a business trip. It only works for the designated PC and the user that the admin sets for the user to logon with a OTP code in advance



5. About Dualauth

Company Info

DualAuth

- DualAuth, LLC. is established by eSTORM Co.,Ltd. in the U.S. in order to provide its mutual authentication and payment technologies globally.

- Website : www.dualauth.com / www.autopassword.com
- Boston Office : 200 Jefferson Rd Suite 107 Wilmington MA 01887
- Phone : +1 (978) 253 4458
- Seoul Office : Namsung Plaza 13F Gumchen-gu Digital-ro, Seoul 34530
- Phone : +82 70 4313 3639
- Email : support@dualauth.com