AutoPassword™

WHITE PAPER

What is AutoPassword™?

VERSION: 2.0
Dated: March 3, 2021

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

Table of Contents

Brief Introduction of DualAuth

We have developed on/offline mutual authentication and access management technologies.
It is the very first mutual authentication technology that allows the user to verify the authenticity of the on/offline service providers before giving their code. Thanks to double security with mutual authentication and convenient usability, we achieved the results shown below in a short period.

1. Major 5 top technical achievements

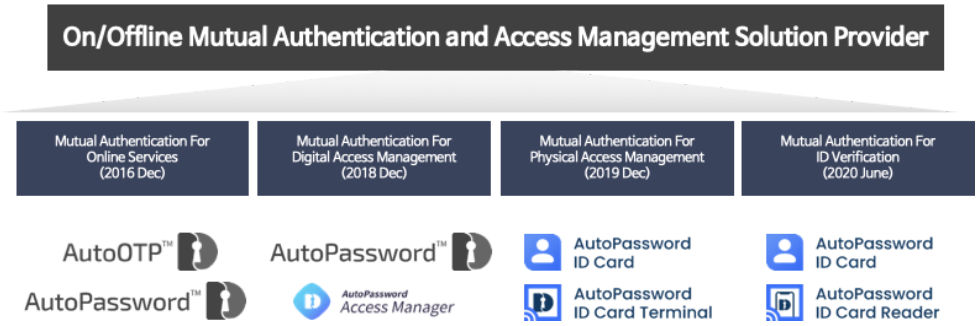
1. IBM Security Partner
2. Gartner mentioned “Well-balanced authentication technology”
3. London Fintech Innovation Awards Top 5 finalist
4. Korea Internet Award’s Ministry Winner
5. The international standards body and trade institution for authentication (Oath and FIDO Association) verified the technology

2. Major 5 top Customers

1. Wooribank (No1. Commercial bank in Korea)
2. Blue house (The Presidential Office of Korea)
3. Online Privacy Association in Korea
4. DDC City government
5. VP (No.1 Online Credit Card Processing Company)

3. Major Product Line

1. AutoOTP
2. AutoPassword
3. AutoPassword Access Manager
4. AutoPassword ID Card & Reader
5. AutoPassword Terminal



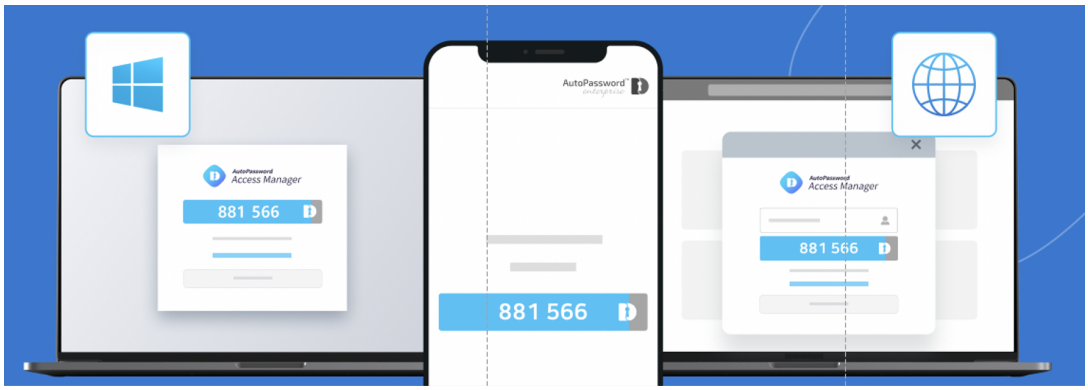
Technical Differentiations of AutoPassword and ID Card

1. User-friendly authentication technology

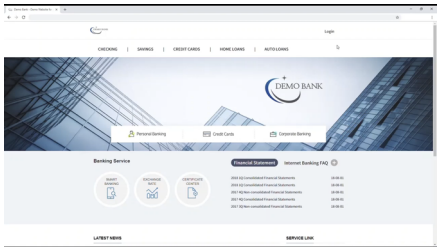
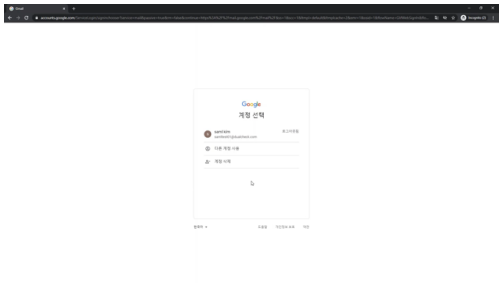
People dislike remembering and inputting the user password when accessing online services and never update their user password.

Instead of asking people to remember and manage the strong user password, we want people to be free from needing passwords by using the automatic password presented by the online services.

Existing systems ask the user to present their user password to an online service and then the online service verifies the user password presented by the user. But with AutoPassword the user verifies the automatic password that is presented by the online service with the code on their smartphone.



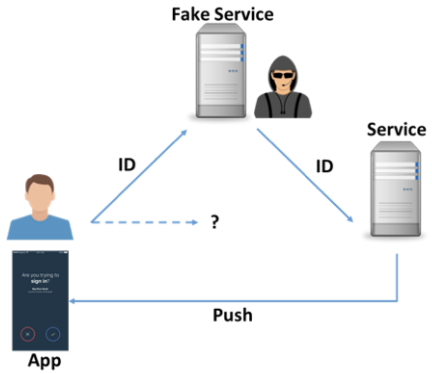
By changing the role of the user from inputting to verifying, people are free from the user password burden. This is good news for the computer illiterate and those without good memory.

Demo for the online service login	Demo for other service login (Gmail)
https://youtu.be/zNMKlIyJ4uU	https://youtu.be/l5H1C9gz7tg
	

2. Mutual Authentication technology

Since the first computer came out in 1961, various types of authentication technologies utilize checking the authenticity of the user only.

In the last 60 years both ICT & cyber crime grew fast. One of the most used cyber attacks is phishing and fake sites. Without knowing that our password was stolen, we face problems if we keep using the same type of password. if we connect the fake online service having the same design, we normally input the user credential. This problem is because of the use-only authentication technology. Using push based mobile authentication technology, the problem is the same. Check out the below diagram.

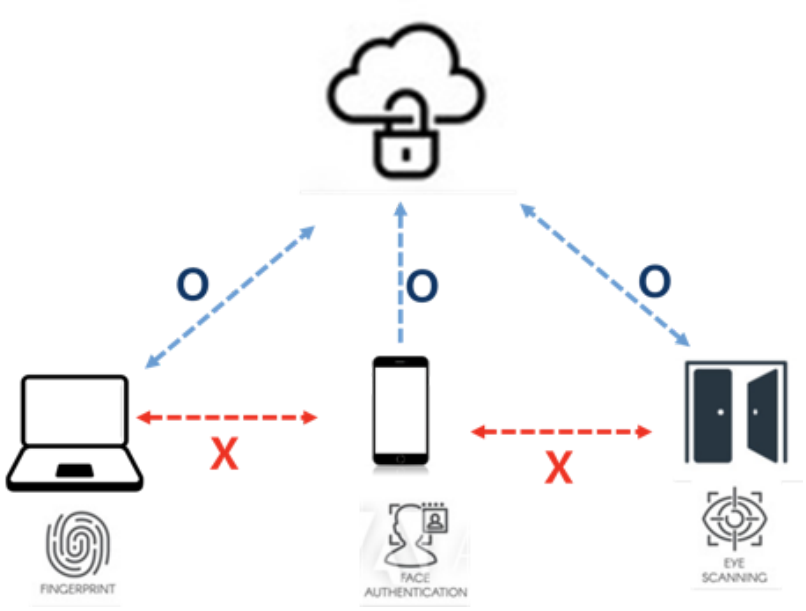


AutoPassword is the first technology which allows the user to verify the authenticity of the online service with their eyes. In addition, the online service verifies the authenticity of the user when the user confirms the two codes match.

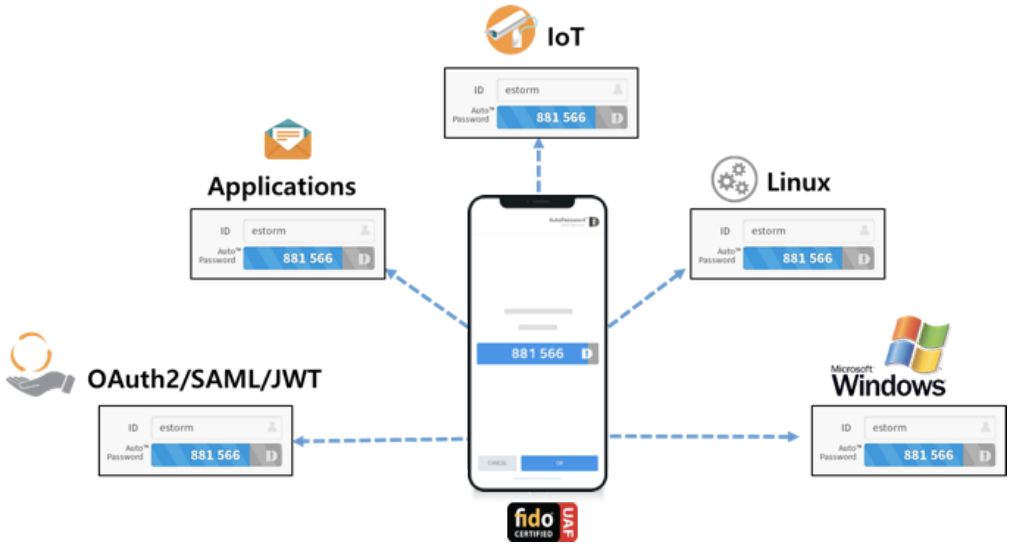
This system does not ignore current user authentication technologies. It uses the same user authentication technology such as OTP, PKI and FIDO biometrics, it does it after verifying the authentication of the service.

3. Crossover biometric authentication technology

AutoPassword uses biometric technology certified by the FIDO (Fast IDentity Online) Alliance. But AutoPassword is unique from the traditional biometric technology for user-only authentication.

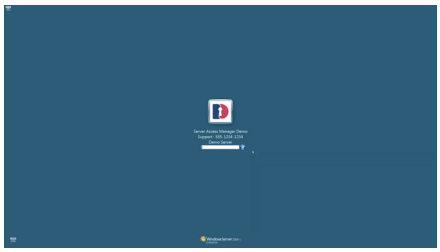


Existing biometric technologies work only on the applications running on the device where the user registers their biometrics. So you cannot use the biometrics registered on your smartphone to the applications running on your PC or AI speaker. Because of that, you have to re-register your biometrics to every device wherever you want to authenticate your biometrics.



By using AutoPassword, you do not need to re-register your biometrics across all devices. You can use your biometrics on your smartphone for each device by presenting the automatic code.

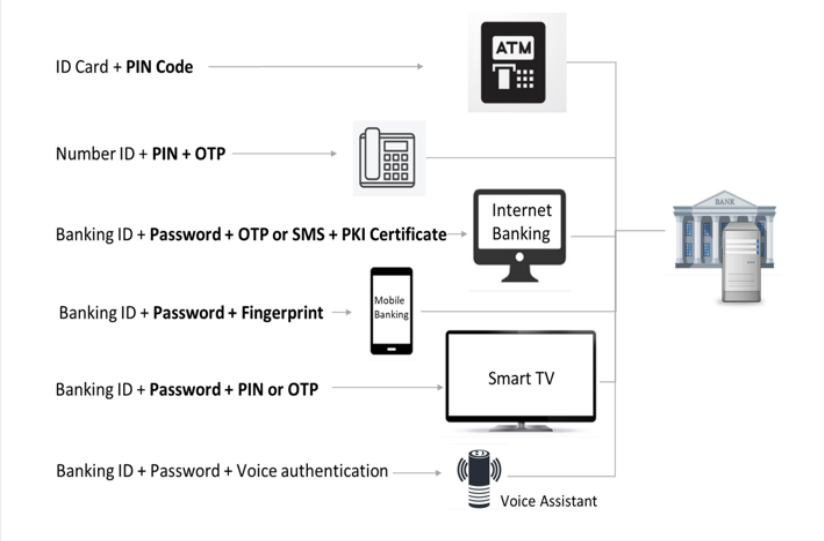
AutoPassword logically links your biometrics on your smartphone to the devices which do not register your biometrics.

Windows Logon Demo	Linux Login Demo
https://youtu.be/cjmjBDwgw00	https://youtu.be/FDt0i06otUI
	

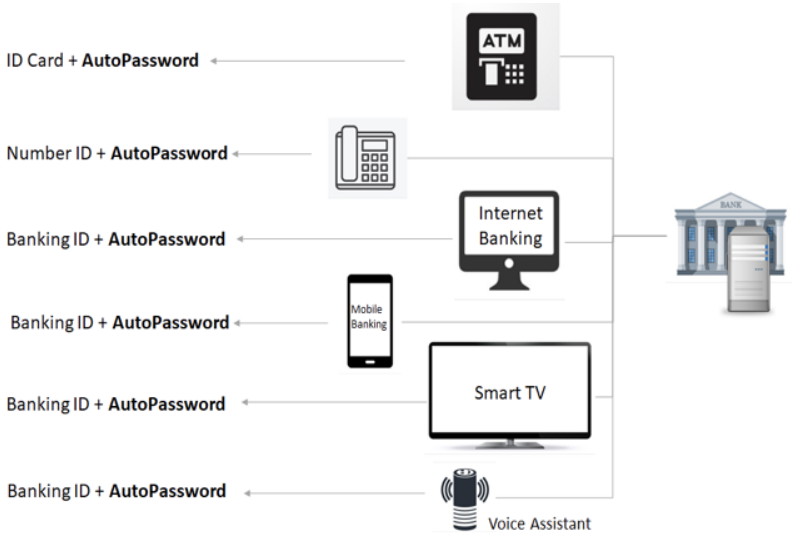
4. Omni-Channel authentication technology

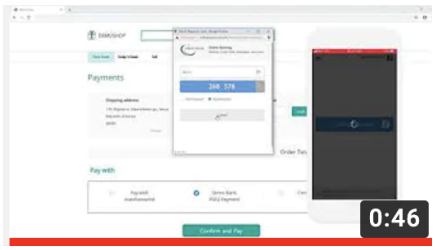
By adding service channels, more authentication methods are required. At a Kiosk or ATM, Card & Pin code are required, using a Mobile device, face recognition or fingerprints are required, using a Smart TV the SMS code or Pin code are required, with an AI speaker, voice authentication is required.

With additional service channels being added, more authentication methods are needed following the device. To simplify things, we need to think out of the box. We can make our life simple by using service-presenting code instead of using a user-presenting credential.



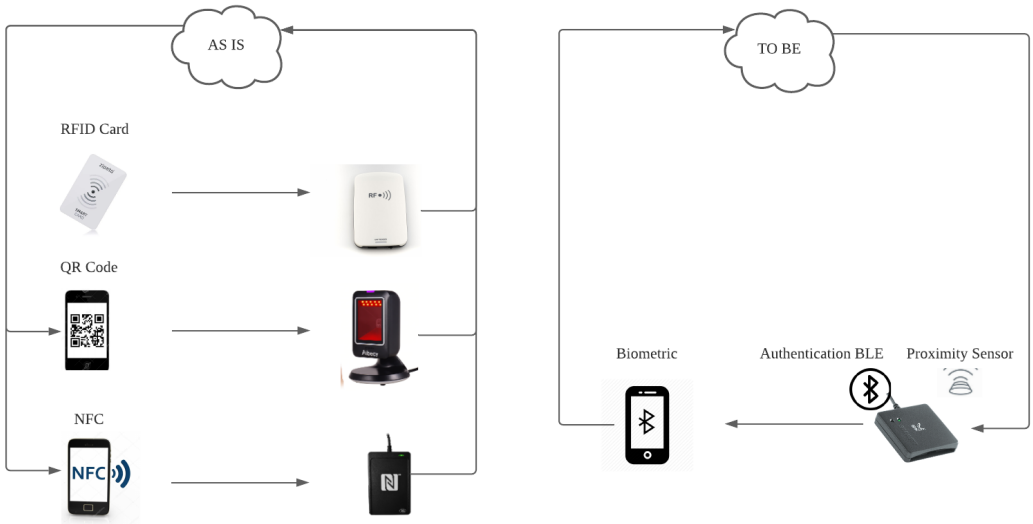
Whatever service channel is in use, by using the AutoPassword presented by the service, it just compares that two numbers match between the one presented by the service and the one on the smartphone.



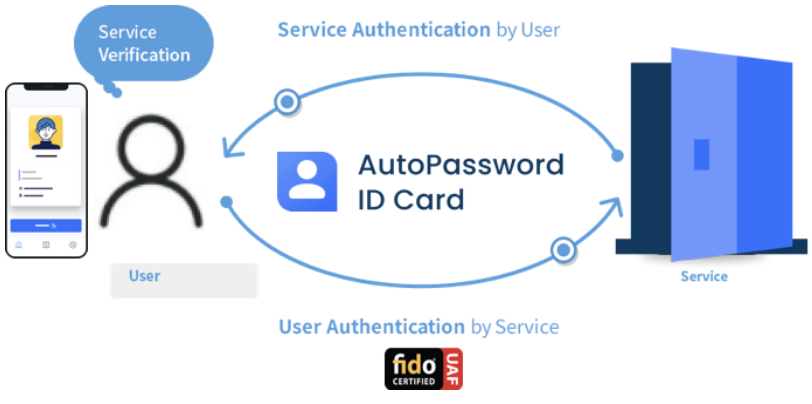
ATM Demo	OpenBanking Demo
https://youtu.be/ytJvOE3f-8k	https://youtu.be/C0rQyXE_3VQ
	

5. On/Offline available authentication technology

After developing the service-presenting AutoPassword technology for online service, we applied the same concept to the offline service. Present the user ID card technology such as magnetic strip, bar code, QR code and RFID chip—they all check the authenticity of the user. By replacing the role of the user from the presenter to the judge, we make our life easier. Check out the diagram below. By changing the authentication direction from the AS IS to To BE, the user can easily combine the authentication method as one mobile app. Example: a user can control the electric facilities such as the automatic door and the light with their AutoPassword ID Card app.



Because it uses the authenticated Beacon, which is Bluetooth frequency with one-time code changing every 60 seconds, it gives the user the ability to check the authenticity of the facility and the manager to see whether the user is in front of the facility.



AutoPassword ID Card also supports a contact and contactless method. So a user can control facilities while being 2 meters away as a non contact method or 1 cm as a contact method. In the contact method, It works like NFC but it allows a user to use both sides of their smartphone as touch side, not only the back side of the phone.

Contact Method Demo	Non-contact method Demo
https://youtu.be/cqWf8bZtdSk	https://youtu.be/oOIUkjsTlZw