AutoPassword™

# WHITE PAPER 1

## What is AutoPassword™?

**VERSION: 1.0**

Dated: Dec 20, 2017

**Prepared By:**

John Woo

David Kim

# 1. What is AutoPassword™ ?

The existing username and password authentication method is vulnerable to theft and leakage. Hackers can easily use phishing and pharming techniques to steal the credentials. Also, as the users tend to use the same passwords to access different online services, security risks are continuously rising.

AutoPassword™ is a password replacement technology that automatically enters passwords for the user. After the password is generated and entered, AutoPassword™ allows the user to verify if the correct password has been entered by showing the generated password on their smartphone. AutoPassword™ cannot be stolen as the password is generated uniquely each time using One-Time-Password technology. In addition to letting the users verify the online service, AutoPassword™ removes the user's need to enter or remember the passwords.


## 2. What are the benefits of using AutoPassword?

AutoPassword™, which allows the user to verify the service provider with their own eyes, provides better security, usability and is more cost effective than all the other existing authentication technologies.

### 2.1 Excellent Security Solution that verifies the service

All the authentication methods out there assume that the connected service is legitimate. The other authentication methods solely exist to verify the user, not the service. Authentication methods such as user/password, SMS, OTP, PKI, and Biometric are vulnerable to hacking since the user is passing some kind of values to the service without verifying the service provider.

The existing mutual authentication methods such as PKI or Kerbros were not invented to verify the service, but instead were invented to prevent the Man-in-the-Middle (MitM) attack. Therefore, the existing mutual authentication technologies solely rely on one-sided machine to machine communication to verify the legitimacy of the user and the devices. There is no human interaction involved in this process to verify the legitimacy of the connected service. In fact, no existing authentication technology in the history has been successful in allowing the users to verify the service legitimacy with their own eyes.

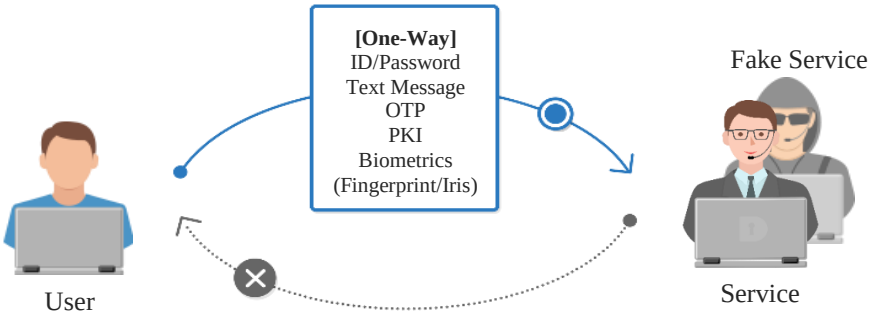
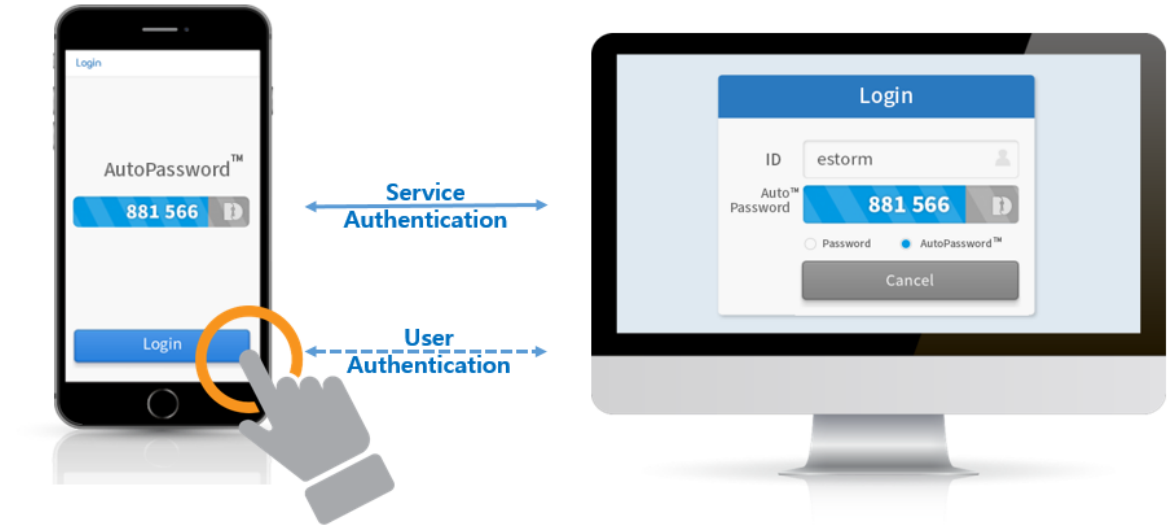



**Figure 1 : Existing One-Way Authentication**

AutoPassword™ is the only authentication solution that can provide a service verification technology. When the user connects to the service, one-time-password is generated and shown on the access page. Same one-time-password will be generated on the service side and users just need to compare the values to verify the service. If the generated passwords match, the user can approve the login to connect to the service. When the user is approving the service, the service also identifies the user using the one-time-password (encrypted with PKI technologies) sent from the user's mobile application. AutoPassword™ is the only mutual authentication technology that explicitly allows both the user and the service to verify each other.

## 2.2 Simple and Effective

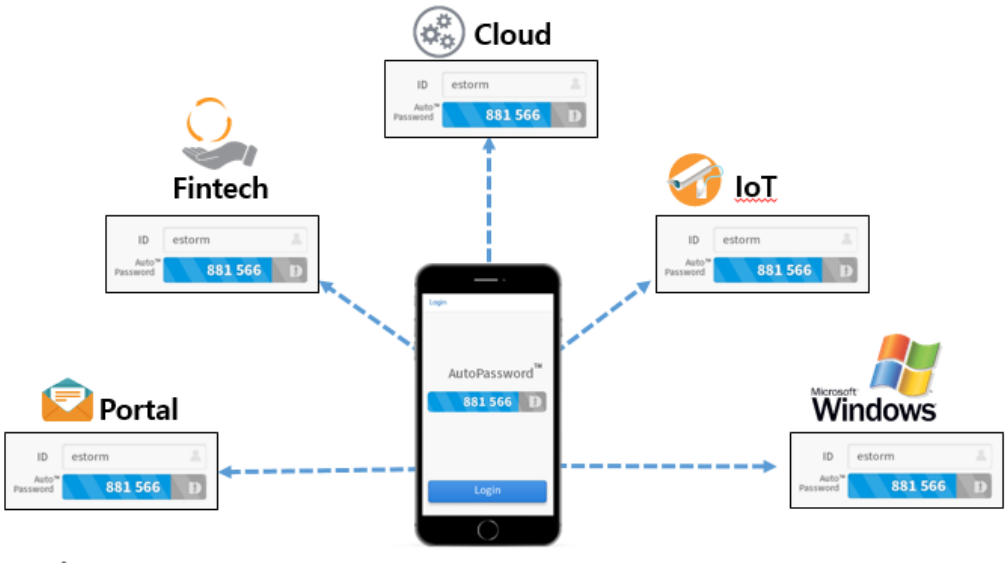
Ironically, the mutual authentication technology of AutoPassword™ uses a very complex algorithm to provide high level of security, but it is very easy to use. Compared to the username / password authentication methods, AutoPassword™ eliminates the need for users to remember, change and enter the password. AutoPassword™ is an adequate solution to resolve the issues associated with user's resistance in using 2 Factor Authentication. Users are more engaged because they are not suggested to add another 2FA solution because their passwords are vulnerable to hacking, but are suggested to implement a solution that resolves the inconvenience of changing, memorizing and entering their passwords.




<Figure 2 : AutoPassword Verifications>

## 1.3 Broad Economic Efficiency

While providing a strong level of security and usability, AutoPassword™ also reduces the costs associated with the authentication. Moreover, AutoPassword™ eliminates the password service calls, which takes up to 30% of the IT service desk call volume. Compared with PKI, FIDO, and Block Chain authenticator, which are the latest authentication technologies using smartphone, AutoPassword™ can connect to different services such as PC, tablet, kiosk and TV. Users can integrate the different authentication methods that had to be implemented for each service terminal into one. AutoPassword™ also has cost advantages against SMS-Based authentication method since it eliminates the communication costs




**Contacts:**


- **John Woo/ CEO**

  jhwoo@AutoPassword.com

- **David Kim / Marketing Lead**

  DKim35@AutoPassword.com