eSTORM

Introduction to AutoPassword™

that automatically creates and enters a password

AutoPassword™

Table of Contents

Inconvenience and vulnerabilities of user password

The existing authentication method where users enter their passwords for online services can be leaked or stolen, and it is vulnerable against phishing or pharming attacks. Also, since users tend to use the same password because it is hard for them to remember each different password when using several various online services, the user authentication based on the user password is not only inconvenient but really vulnerable against security threats.

Phishing

Pharming

Memorizing Passwords

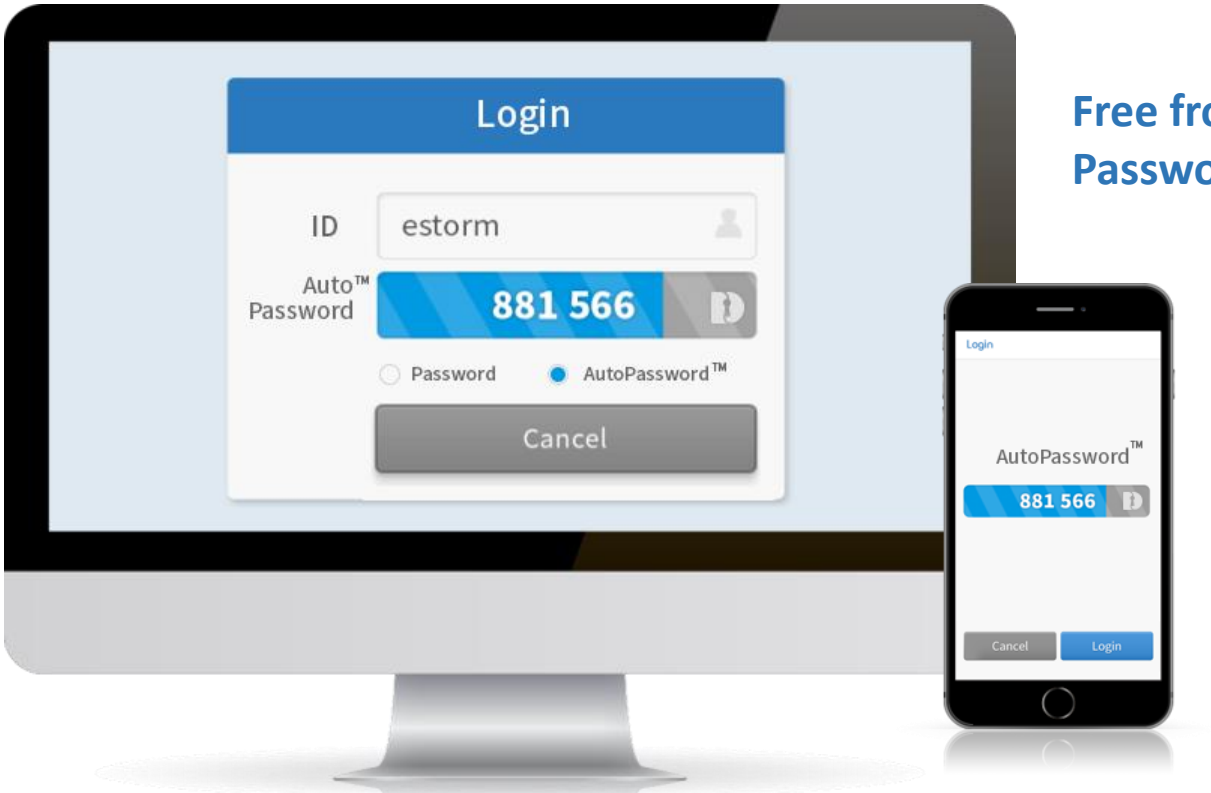
Entering Passwords

Magical service that automatically generates and enters a password for you

It is the password replacement technology that automatically enters a password for the user when the user enters his or her ID on the online service, and verifies whether the correct password is entered to the service on the smartphone. AutoPassword™ cannot be stolen as it is being created newly every time powered by the AutoPassword™ technology, users don't have to annoyingly memorize or enter passwords, and it verifies whether the online service is normal, not a pharming site.

Prevent Phishing

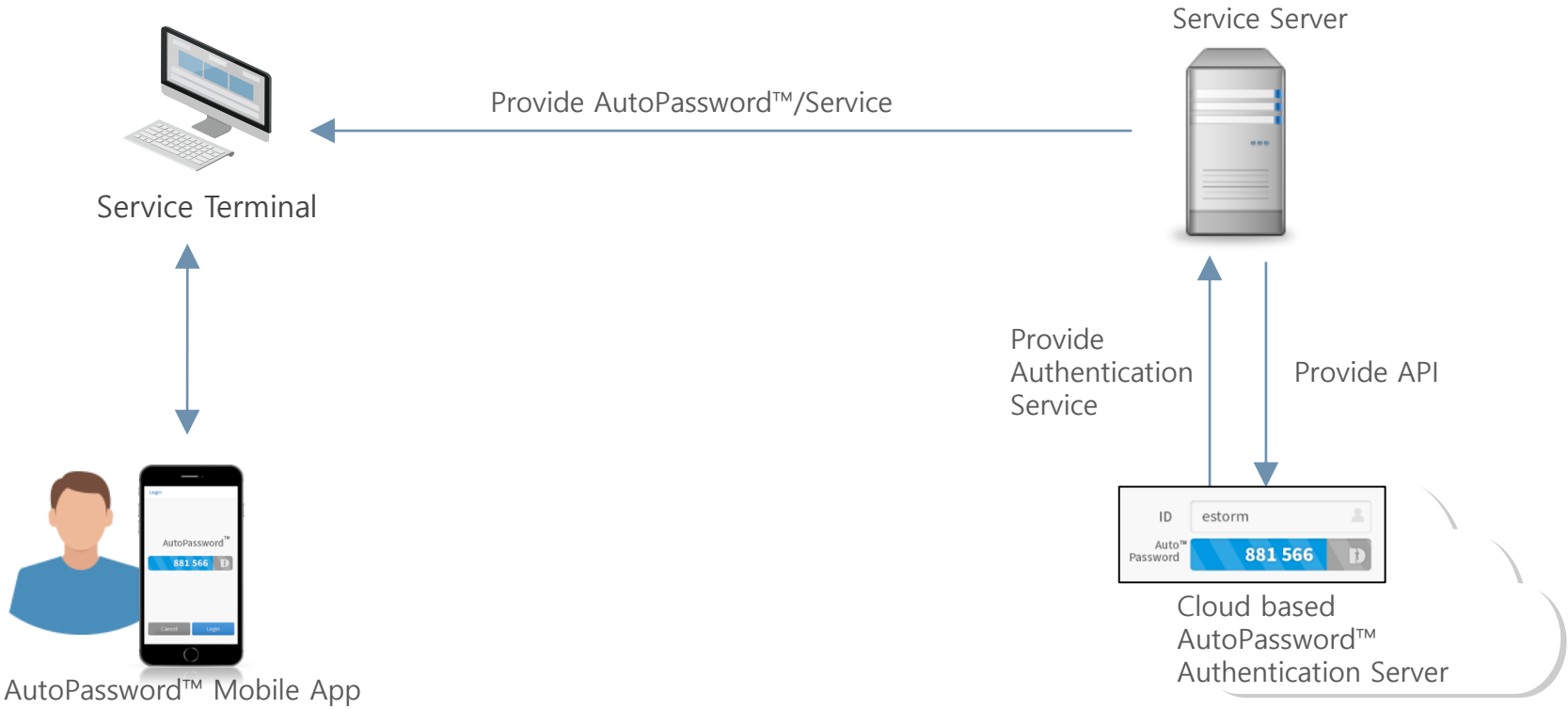
Prevent Pharming



Free from Password

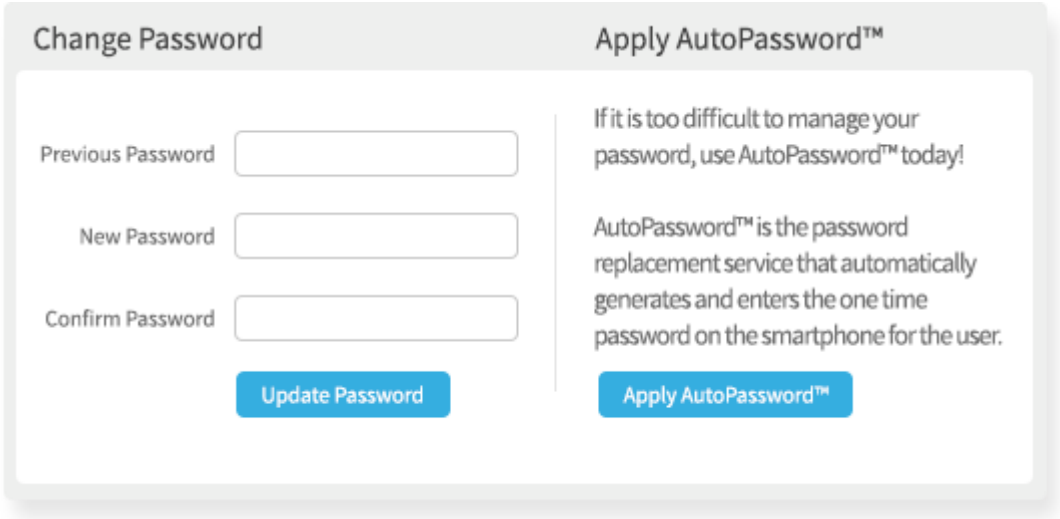
3-1 Adding an AutoPassword™ mobile app and authentication server to the existing online services

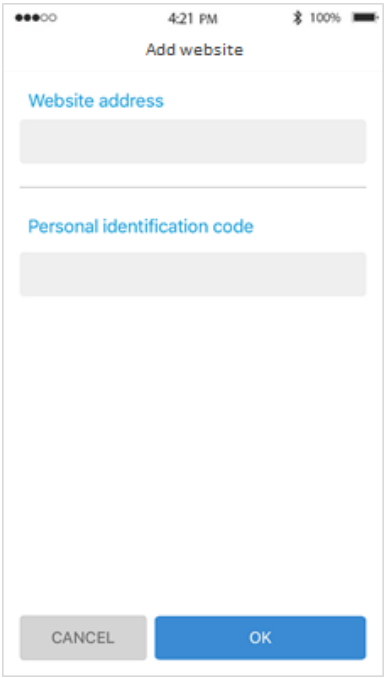
AutoPassword™ consists of the AutoPassword™ server that provides the automatic password service as being connected with the online service server and the AutoPassword™ mobile app that verifies the AutoPassword™ on the user's smartphone. AutoPassword™ provides various APIs so that the existing service server can be smoothly connected with the AutoPassword™ authentication server.



3-2 AutoPassword™ registration phase

To use AutoPassword™, it is required to add the AutoPassword™ registration page to the password change menu of the online service, and to issue the user verification number after receiving a user's agreement of using AutoPassword™. AutoPassword™ doesn't get any personally identifiable information of the service user except the personal identification code. This randomly generated value according to the online service policy can be issued directly on the service screen, or delivered through SMS or emails. The users can use the AutoPassword™ service when they register the service domain, and user verification number by downloading the AutoPassword™ app.

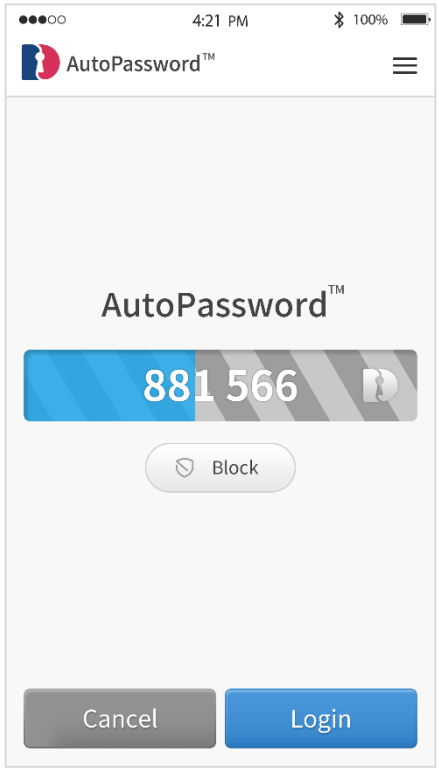




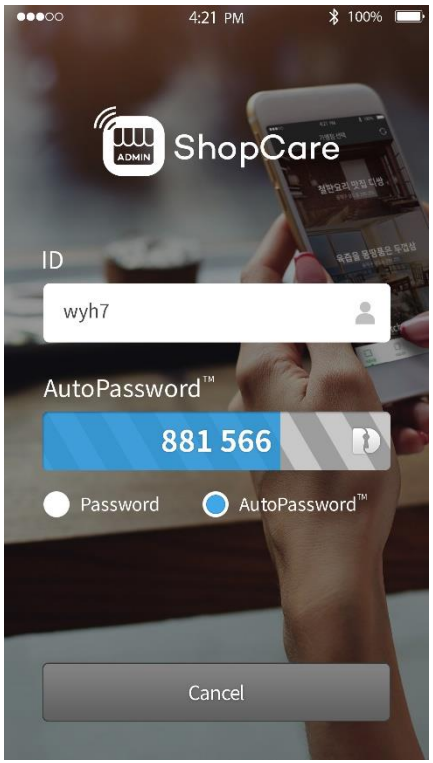
3-3 AutoPassword™ authentication phase

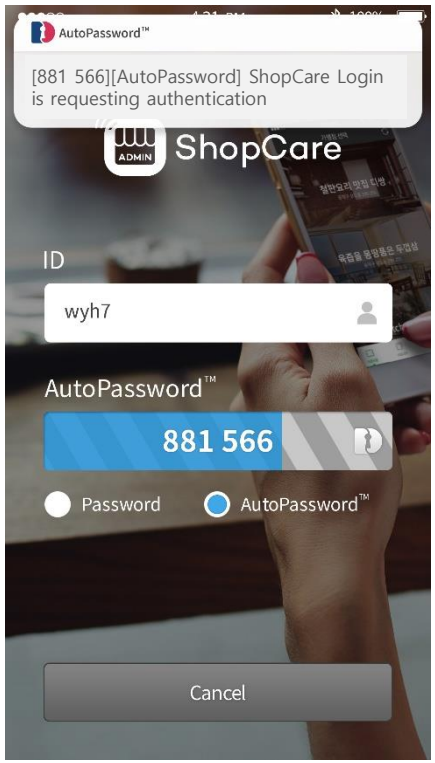
AutoPassword™ automatically works when the user enters ID by accessing the user's PC or mobile service. As soon as the user enters ID, AutoPassword™ is generated on the smartphone, and the only thing the user has to do is verify whether AutoPassword™ displayed on the push message and AutoPassword™ displayed on mobile match without having to unnecessarily switch to different mobile app screens.

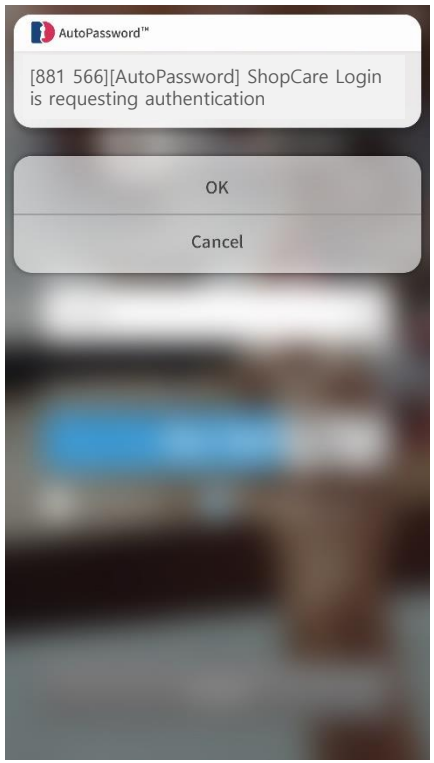
PC Demo



Mobile App Demo

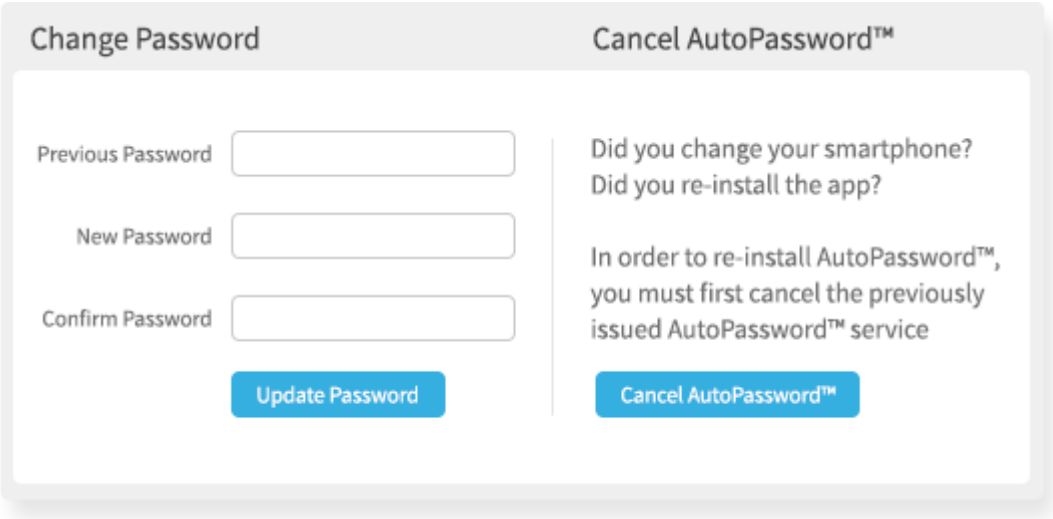






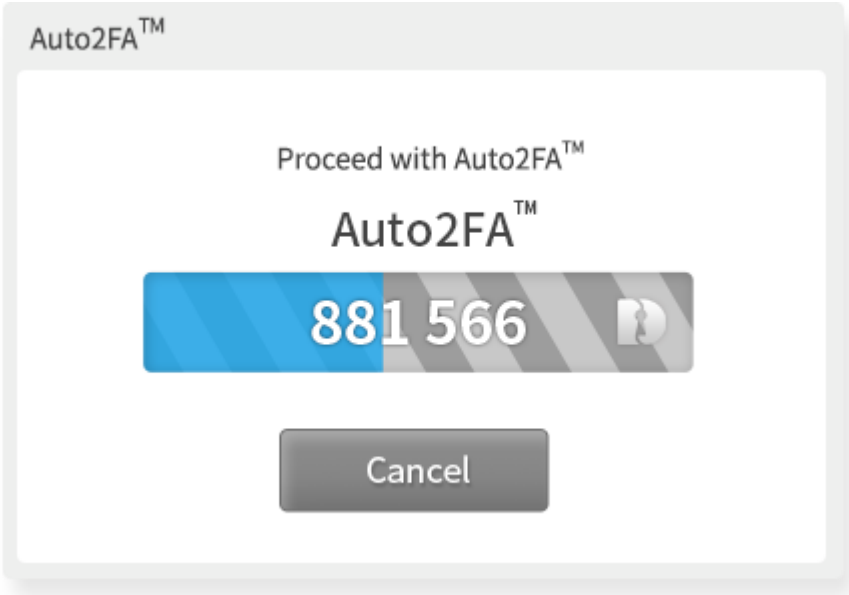
3-4 AutoPassword™ deactivation phase

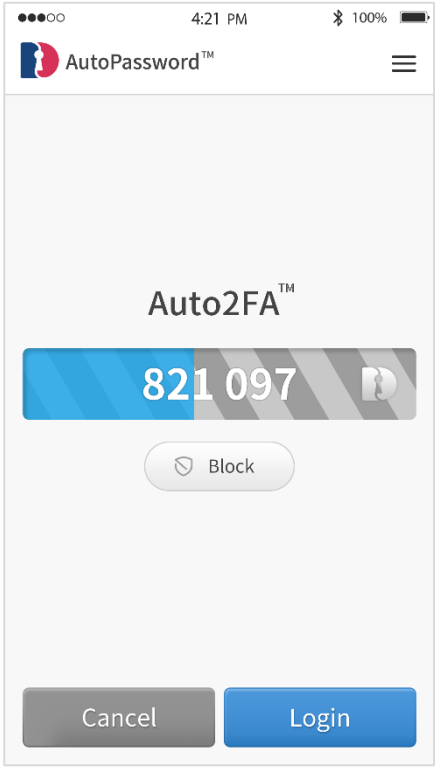
The user can deactivate the AutoPassword™ service anytime on the service screen. When the user click the deactivate button on the existing AutoPassword™ deactivation page, the information about how to deactivate AutoPassword™ will be delivered to the corresponding smartphone. The users must re-register after deactivating the existing service if they change their smartphones or have to re-install a new AutoPassword™ app.



3-5 The method of application of Auto2FA™ for social login

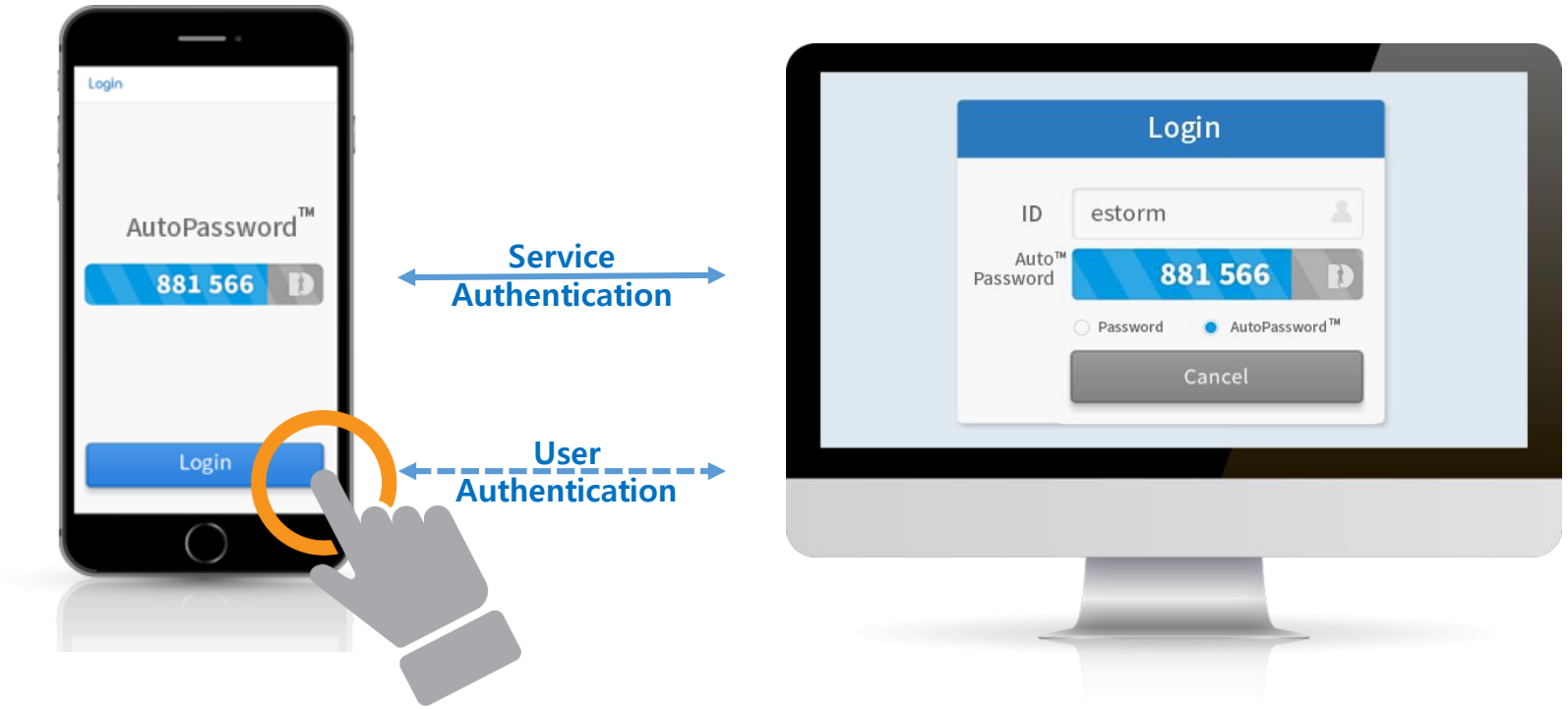
AutoPassword™ can be set to run the automatic Two-Factor Authentication(Auto2FA™) after social logging in to the online service applied with the social login service. Even though the user's social login service ID and password are stolen, the Auto2FA™ service safely protects the user account. When the users log in through social login, Auto2FA™ is automatically displayed on the screen and they are able to process Auto2FA™ on their smartphones.





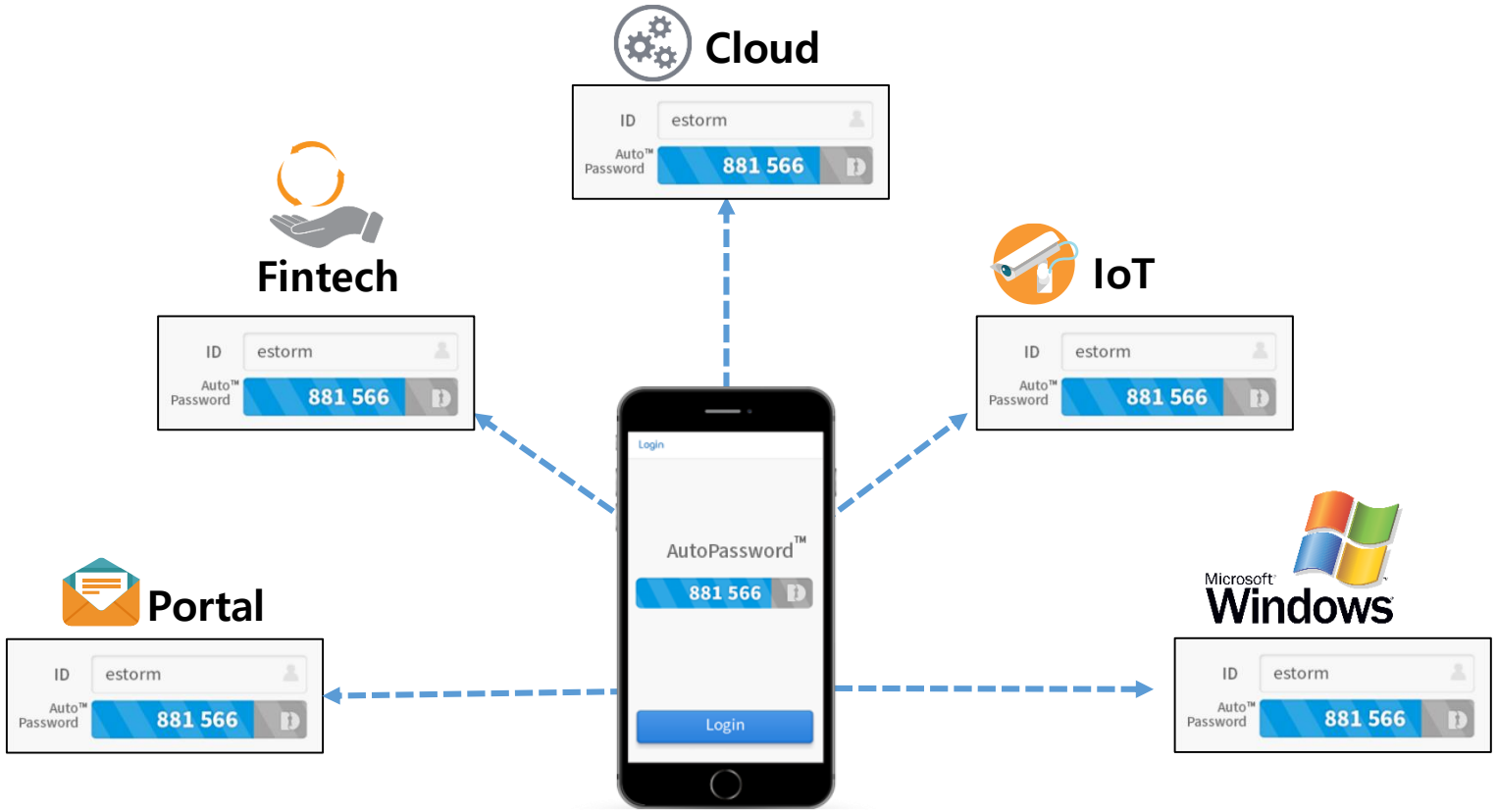
4-1 DualAuth technology that verifies both the user and the service

It allows the users verify the service providers through their smartphones by the service automatically displaying the one time password when the users enter their IDs. It is also a mutual authentication technology that when the users verify the service's one time password, the user's one time password is generated internally and delivered to the service, and the service also verifies the user's one time password. Among all current authentication technologies, it is the only technology that the user can explicitly verify the service.



4-2 Replace various user passwords with one AutoPassword™

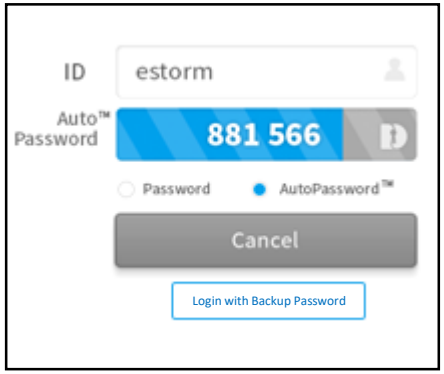
With AutoPassword™, the users don't have to remember or enter user passwords for each different service that they use. Since the AutoPassword™ service is immediately provided when the authentication server is connected with the service server, the customers can conveniently use the service without the burden of the user password no matter how many services they use.



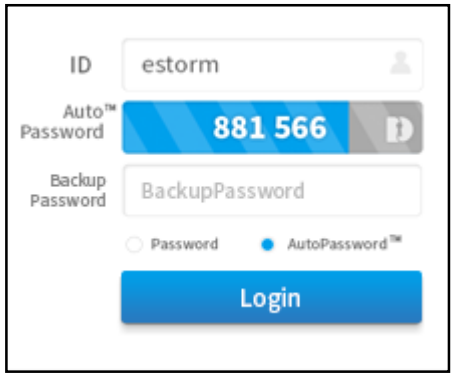
4-3 Flexibility in case of losing a smartphone

AutoPassword™ provides a user password function and an additional backup code, considering the situation where the user cannot use the smartphone due to its loss or impediment. The admin can allow users to use the service by the existing user password in a situation where they don't have smartphones, or set it up to use the service by issuing an additional backup password.

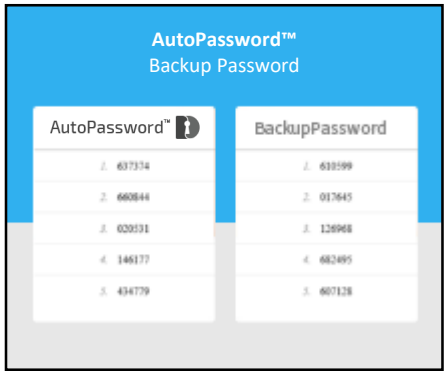
Admin



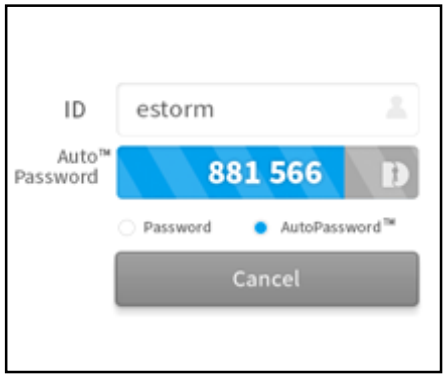
Backup Password Login



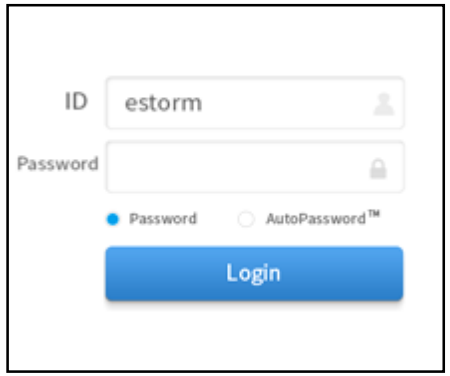
Enter Backup Password



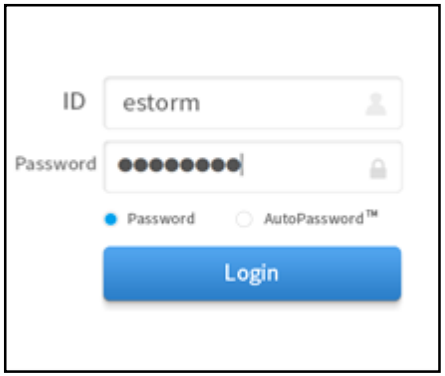
Issued Backup Password



Change login to User Password



User Password Login



Enter User Password

4-4 The password service with the world best security authentication technologies

AutoPassword™ is integrated with the world's best security authentication technologies along with its excellent usability. AutoPassword™ is applied with the world's top class security authentication technology since the service password technology that the user can verify the service, biometric authentication technology and the international standard FIDO combined with the PKI authentication technology, and the geographic location-based authentication technology that verifies the user by verifying the IP address accessed by the user, are all applied together. AutoPassword™ has received attention from Gartner, IBM, and the global tech competitions in places such as New York, Hong Kong, London, Tokyo, and Seoul.

Gartner Report
Don't Waste Time and Energy Tinkering With Password Policies; Invest in More Robust Authentication Methods or Other Compensating Controls
27 July 2017 ID: G00326733 Ant Allan

Security Intelligence News
IBM Security Expands Partner Ecosystem for Multifactor Authentication
https://securityintelligence.com/news/ibm-security-expands-partner-ecosystem-for-multifactor-authentication/

NEW YORK	HONG KONG	LONDON	TOKYO	SEOUL
				
Selected as FinovateFall 2016 Presenter	Selected as FinovateAsia 2016 Presenter	Selected as FinTech Innovation Awards 2016 Finalist	Selected as NTT Data Innovation 2017 Finalist	Selected as Korea Internet Grand Prize Winner

Company & Business Overview

DualAuth

- DualAuth, LLC. is established by eSTORM Co.,Ltd. in the U.S. in order to provide its Automatic Mutual Authentication technology globally.
- Website : www.dualauth.com / www.autopassword.com
- Address : 280 Worcester Rd Suite 102 Framingham, MA 01702
- Email : sales@autopassword.com

eSTORM

- Company : eSTORM Co.,Ltd.
- Mission : Helping People Do the Right
- Established in : 1999
- Address : 130 Digital-ro, Suite 1310 ~ 1311, Geumcheon-gu, Seoul 08589
- Email : sales@estorm.co.kr