

AutoPassword™ 소개서

자동으로 암호를 생성하고 입력해주는 서비스



01 사용자 암호의 문제점

02 AutoPassword™ 개요

03 AutoPassword™ 운영

04 AutoPassword™ 특징점

05 DualAuth 소개

사용자 암호의 불편함과 취약함

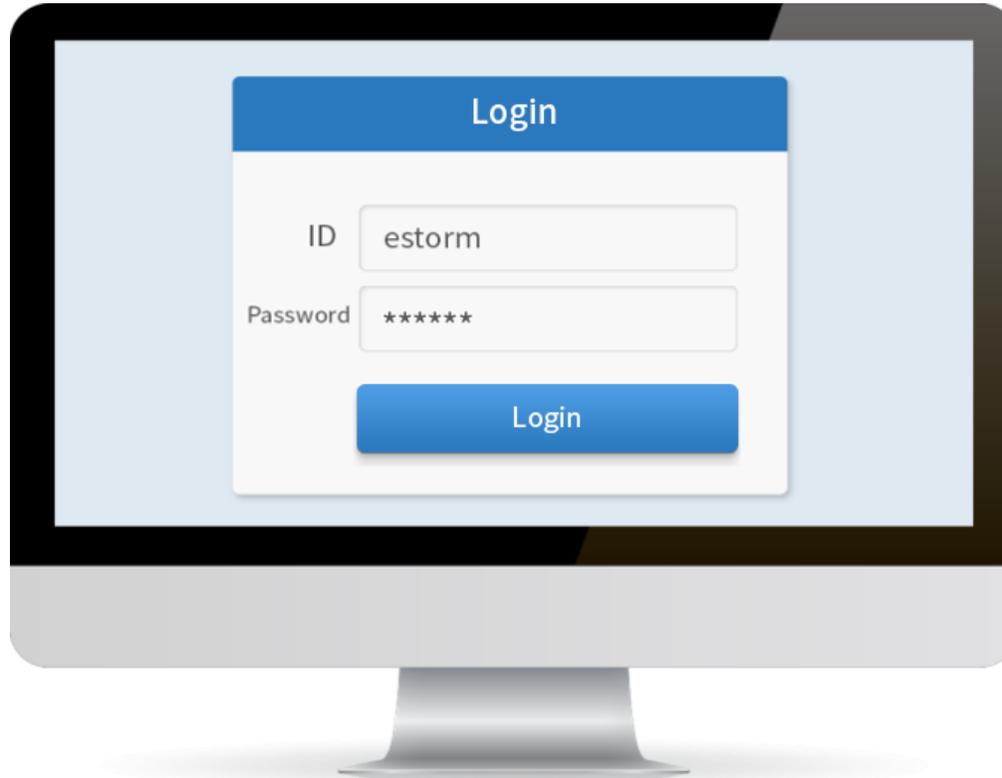
사용자가 온라인 서비스에 사용자 암호를 입력하는 기존 인증 방식은 암호가 도용되거나 유출될 수 있으며, 항상 해커의 피싱이나 파밍공격에 취약합니다. 또한 다양한 여러 온라인 서비스를 사용할 때 각각의 사용자 암호를 숙지하기도 어려워 동일한 암호를 사용하게 되기 때문에 사용자 암호는 불편할 뿐만 아니라 보안에 취약합니다.



피싱



파밍



암호숙지



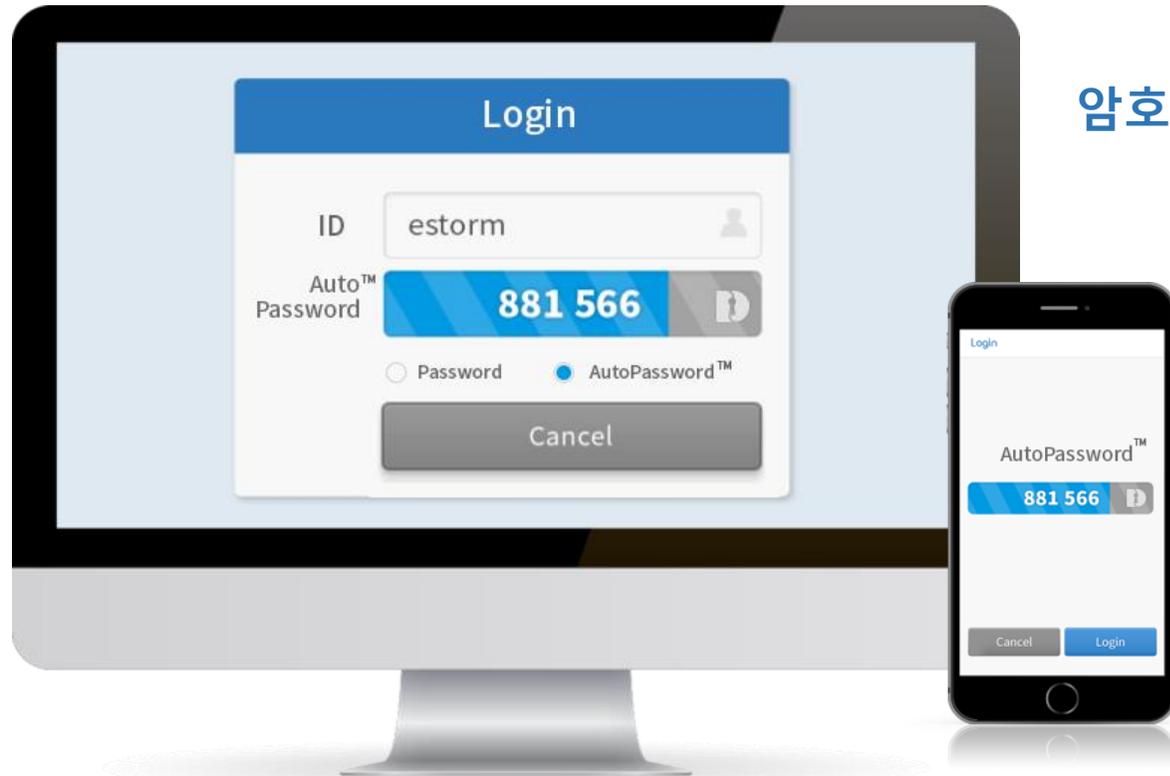
암호입력

자동으로 암호를 생성하고 입력까지 해주는 마법 같은 서비스

온라인 서비스에 사용자가 아이디를 입력하면 사용자를 대신하여 자동으로 암호를 입력해주고, 사용자에게 올바른 암호가 입력되었는지 스마트폰에서 확인시켜주는 사용자 암호 대체 기술입니다. 매번 새롭게 생성되어 도용될 수 없으며, 사용자가 귀찮게 외우거나 입력할 필요도 없고, 온라인 서비스가 파밍되지 않은 정상적인 서비스인지까지 확인시켜 줍니다.

피싱 예방

파밍 예방



암호 해방

3-1 인증 서버와 모바일 인증 앱

온라인 서비스 서버에 연결되어 AutoPassword™ 서비스를 제공해주는 인증 서버와 사용자의 스마트폰에서 AutoPassword™를 확인시켜 주는 모바일 인증 앱으로 구성되어 있습니다. 기존 서비스 서버가 클라우드 기반의 인증 서버에 원활히 연동될 수 있게 다양한 연동 API를 제공합니다.



3-2 배포 단계

고객에게 AutoPassword™ 설정 기능을 제공하기 위해 온라인 서비스의 계정 관리 화면 등에 설정 페이지를 추가하고, 사용자의 사용 동의를 받은 후 일회용 본인 확인 코드를 발급해주면 됩니다. 서비스 이용자의 어떠한 개인 식별정보도 받지 않습니다. 온라인 서비스의 정책에 따라서 본인 확인 코드를 온라인 서비스 화면에서 직접 제공할 수도 있고, 문자 메시지나 이메일 등으로 전달될 수도 있습니다. 사용자는 모바일 인증 앱을 다운로드 하여 웹사이트 주소, 본인 확인 코드를 이용하여 웹사이트를 추가하면 해당 서비스에서 AutoPassword™ 서비스를 사용할 수 있습니다.

비밀번호 변경

이전 비밀번호

새 비밀번호

비밀번호 확인

비밀번호 업데이트

AutoPassword™ 설정

비밀번호 관리가 힘들다면
AutoPassword™를 사용하세요!

사용자 대신 스마트폰에서
일회용 비밀번호를 생성하고 입력해주는
비밀번호 대체 서비스입니다.

시작하기

4:21 PM 100%

웹사이트 추가

웹사이트 주소

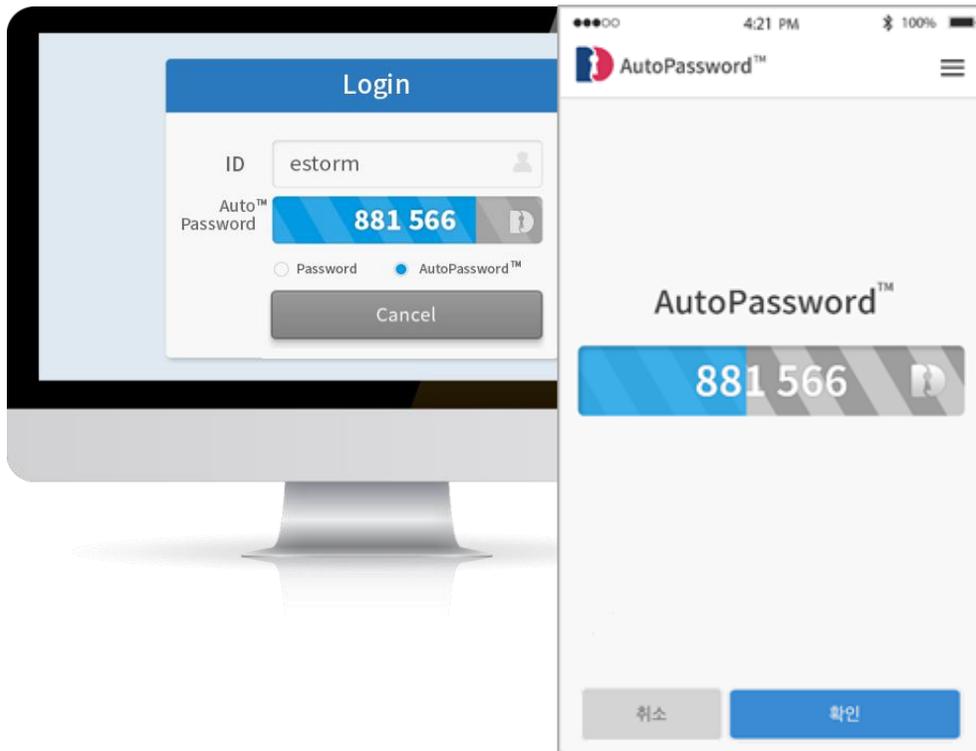
본인 확인 코드

취소 **확인**

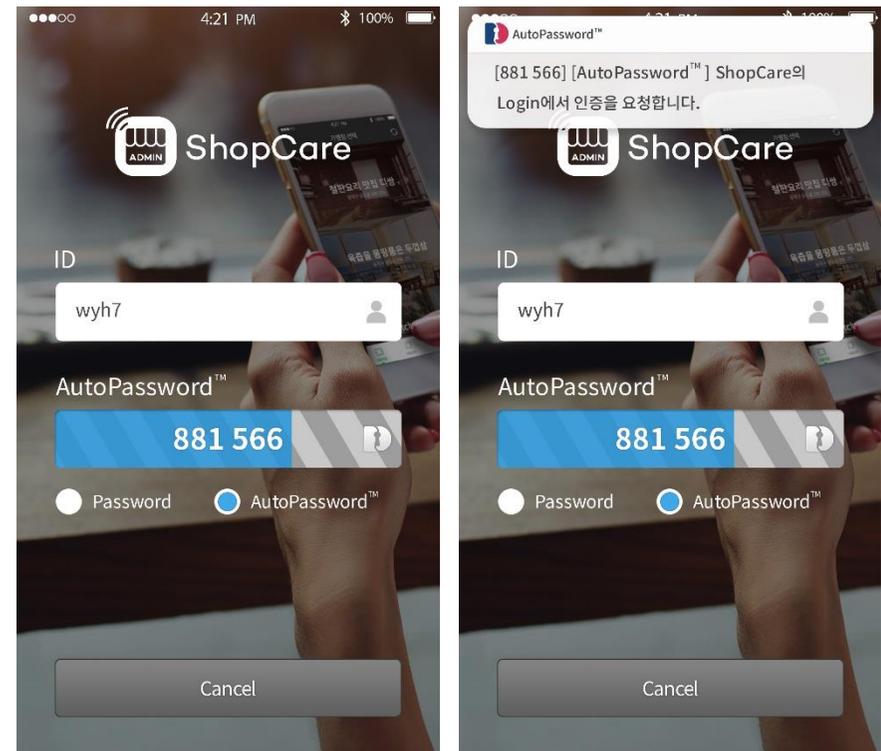
3-3 AutoPassword™ 인증 단계

사용자가 PC나 모바일 서비스에 접속하여 아이디를 입력하면 자동으로 작동합니다. 사용자가 아이디를 입력하면 모바일 인증 앱에서 일회용 암호가 생성되며, 모바일 서비스에서는 번잡하게 화면을 전환할 필요 없이 모바일 앱에 표시된 일회용 암호와 스마트폰 알림 메시지에서 표시되는 일회용 암호가 일치하는지 확인하면 됩니다.

PC 시연



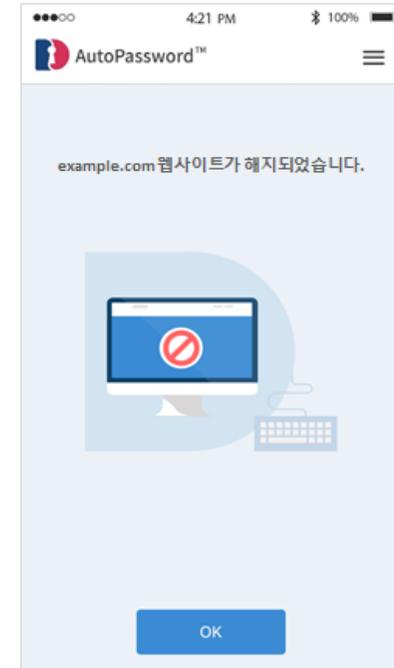
Mobile app 시연



3-4 AutoPassword™ 폐기 단계

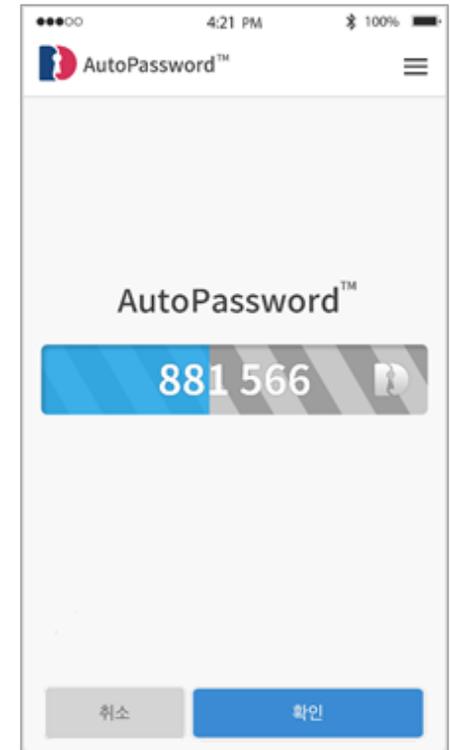
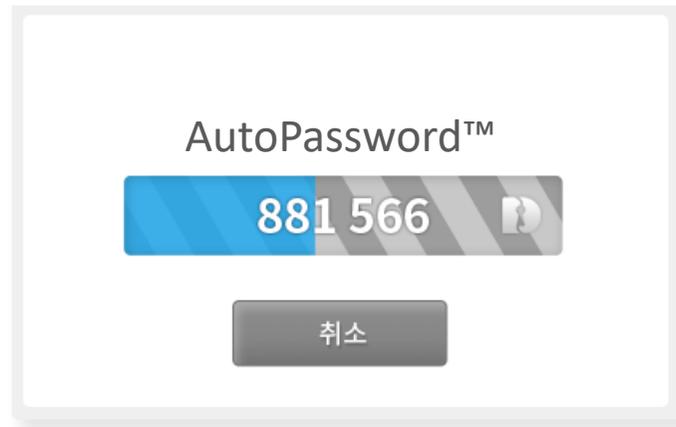
사용자는 언제든지 온라인 서비스 화면에서 이용자가 직접 해지할 수 있습니다. 기존 AutoPassword™ 설정 화면에서 제공되는 해지 기능을 이용하여 설정을 해지합니다. 스마트폰을 교체, 분실 등으로 인해 모바일 인증 앱을 재설치한 경우에는 해지 후 재설정을 해야합니다.

비밀번호 변경	AutoPassword™ 설정
이전 비밀번호 <input type="text"/>	AutoPassword™ 사용 중입니다. 스마트폰 교체, 분실 등에 의해 앱을 재설치한 경우에는 해지 후 재설정이 필요합니다.
새 비밀번호 <input type="text"/>	
비밀번호 확인 <input type="text"/>	
<input type="button" value="비밀번호 업데이트"/>	<input type="button" value="해지"/>



3-5 소셜 로그인에 대한 2차 인증 적용 방식

소셜 로그인 서비스가 적용된 온라인 서비스에서 소셜 로그인 이후 2차으로 AutoPassword™를 설정할 수 있습니다. 사용자가 소셜 로그인 서비스의 아이디와 암호가 탈취된 경우에도 온라인 서비스의 계정을 안전하게 보호합니다. 사용자가 소셜 로그인을 통해서 로그인하게 되면 AutoPassword™가 자동으로 온라인 서비스 화면에 표시되고 사용자는 스마트폰에서 2차 인증을 진행 할 수 있습니다.



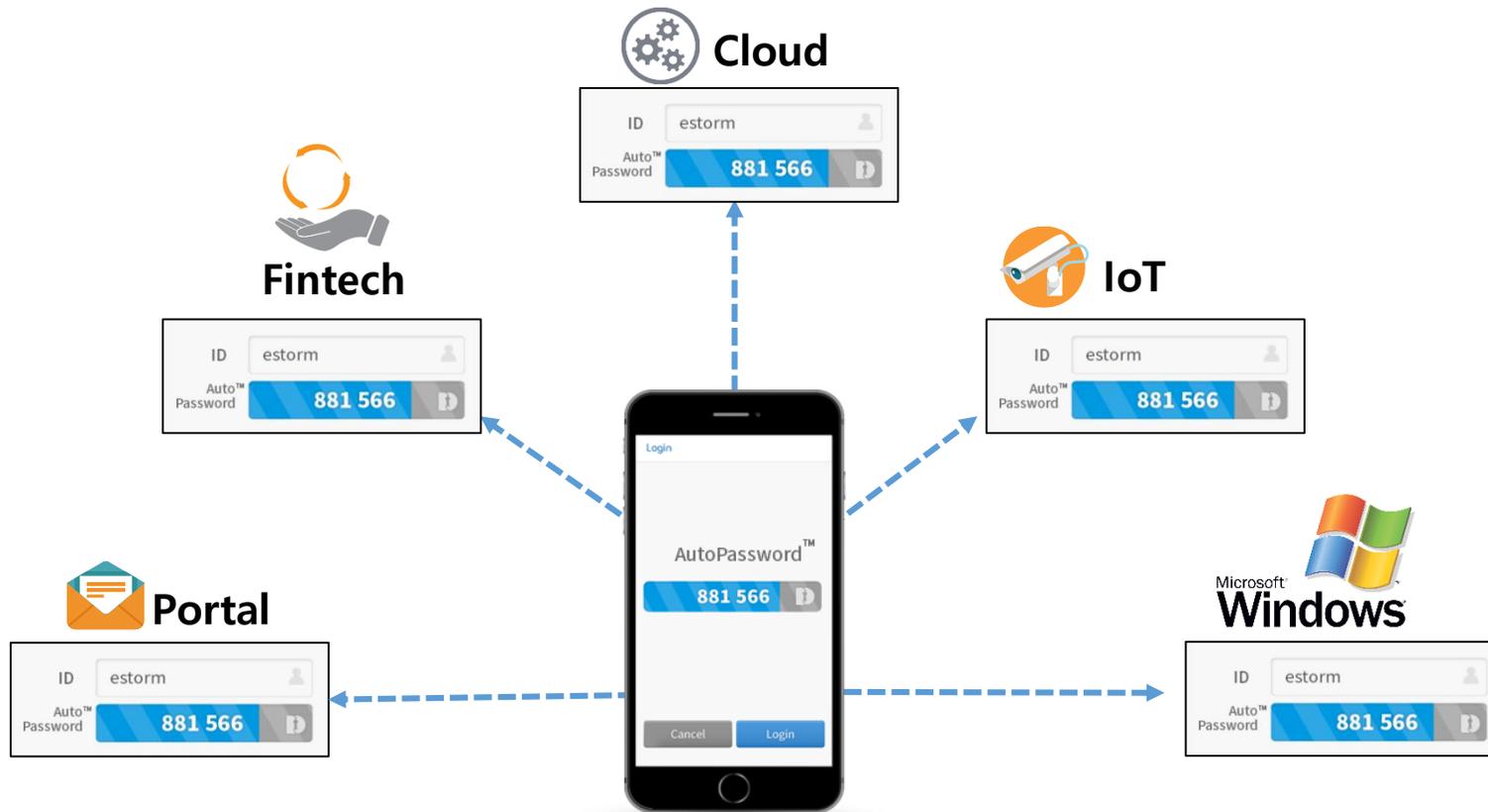
4-1 사용자와 서비스를 동시에 확인하는 DualAuth 기술

사용자가 아이디를 입력하면 서비스가 자동으로 일회용 암호를 표시하여 사용자가 스마트폰으로 서비스 제공자를 확인할 수 있게 하며, 사용자가 서비스의 일회용 암호를 확인할 때 내부적으로 사용자의 일회용 암호를 생성하여 서비스에 전달하고 서비스 역시 사용자의 일회용 암호를 확인하는 상호인증 기술입니다. 현존하는 상호인증 기술 중 사용자가 명시적으로 서비스를 확인할 수 있는 유일한 기술입니다.



4-2 여러 사용자 암호를 하나의 AutoPassword™로 대체

사용자가 이용하는 여러 서비스마다 사용자 암호를 기억하거나 입력할 필요가 없으며, AutoPassword™ 인증 서버와 서비스 서버를 연결하면 그 즉시 AutoPassword™ 서비스가 제공되기 때문에 아무리 많은 서비스를 고객이 이용한다 하더라도 고객이 암호에 대한 부담 없이 편리하게 서비스를 이용할 수 있습니다.



4-3 스마트폰 분실을 대비한 유연성

사용자가 스마트폰을 분실하거나 장애로 사용할 수 없는 상황을 고려하여 기존 사용자 암호와 백업 패스워드 기술을 제공합니다. 서비스 운영자는 사용자가 핸드폰이 없는 상황에서도 서비스를 이용할 수 있도록 기존 사용자 암호로 서비스를 이용할 수 있게 하거나, 별도의 백업 패스워드를 발송하여 서비스를 이용할 수 있게 설정할 수 있습니다.



관리자

백업 패스워드로 로그인

백업 패스워드 입력

AutoPassword™	BackupPassword
1. 637374	1. 638599
2. 660844	2. 017645
3. 020391	3. 126968
4. 146177	4. 682495
5. 434779	5. 607128

발급된 백업 패스워드

로그인 방식을 사용자 패스워드로 변경

사용자 패스워드 로그인 선택

사용자 패스워드 입력

4-4 세계 최고의 보안인증 기술이 집약된 패스워드 서비스

뛰어난 사용성 뿐만 아니라 세계 최고 수준의 보안인증 기술이 집약되어 있습니다. 서비스 제공자를 사용자가 확인 할 수 있는 서비스 패스워드 기술, 생체인증 기술과 PKI 인증 기술이 결합된 국제 표준 FIDO, 사용자가 접속한 상황의 IP주소를 확인하여 본인 여부를 확인하는 지역 기반 인증 기술, 모바일 앱의 위변조를 탐지기술 등이 적용되어 세계 최고 수준의 보안 인증 기술을 적용했습니다.

뉴욕, 홍콩, 런던, 도쿄, 서울 등에서 열린 세계적인 기술 경연장에서 좋은 호평을 받았으며, 2017년 Gartner 인증기술 트렌드 보고서에서 Well Balanced Authenticator로 다시 한번 지목 받았으며, IBM사의 Security 파트너로 등록 되었습니다.

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



Selected as FinovateFall 2016 Presenter

HONG KONG



Selected as FinovateAsia 2016 Presenter

LONDON



Selected as FinTech Innovation Awards 2016 Finalist

TOKYO



Selected as NTT Data Innovation 2017 Finalist

SEOUL



Selected as Korea Internet Grand Prize Winner



기업 및 사업 소개



- 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



- 회 사 명 : (주)이스툼
- 미 선 : 사용자가 올바르게 행동 할 수 있게 돕는다.
- 설 립 일 : 1999년 12월
- 주 소 : 서울특별시 금천구 디지털로 130 남성프라자 13층
- 전 화 : 02-2026-0290