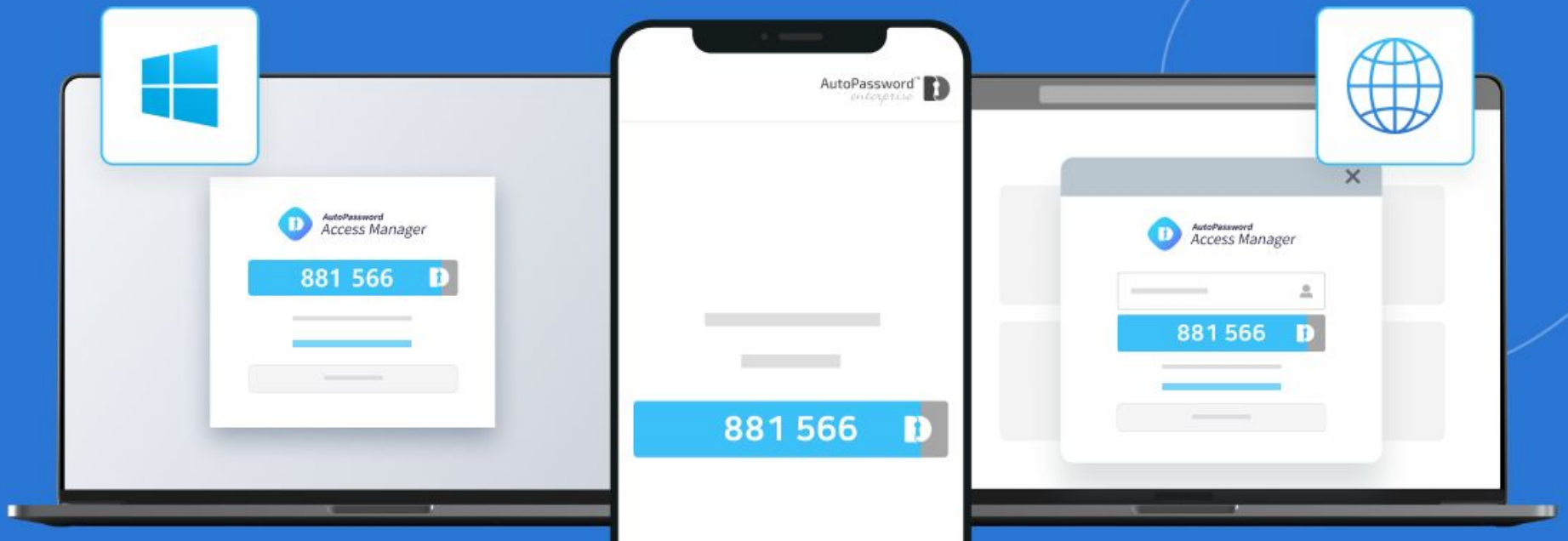
DualAuth

AutoPassword Access Manager

PC 및 업무시스템 통합 자동인증 솔루션 – AutoPassword Access Manager

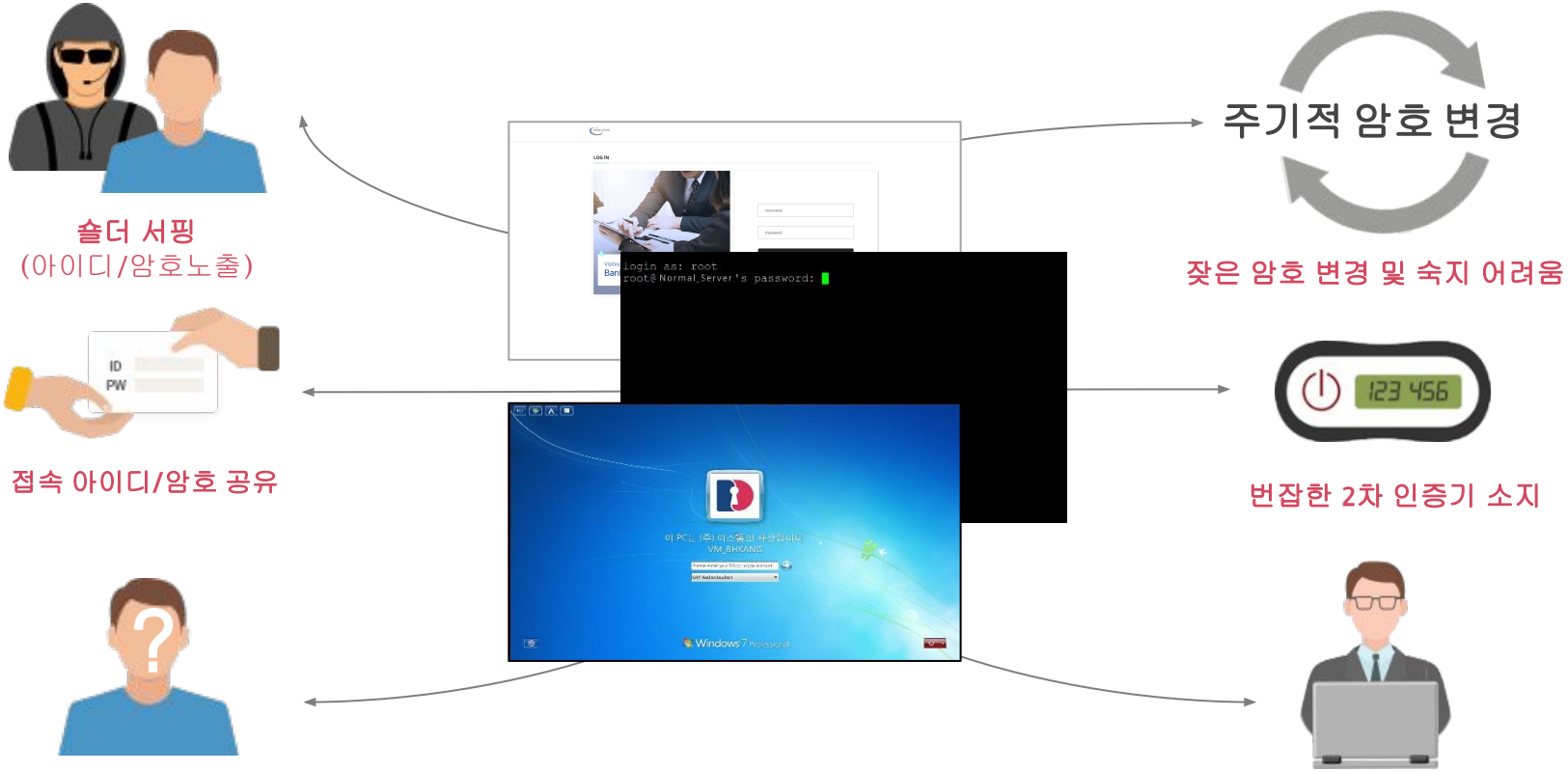
“오토패스워드 액세스 매니저“ 소개



01 암호 관리 현황 및 문제점

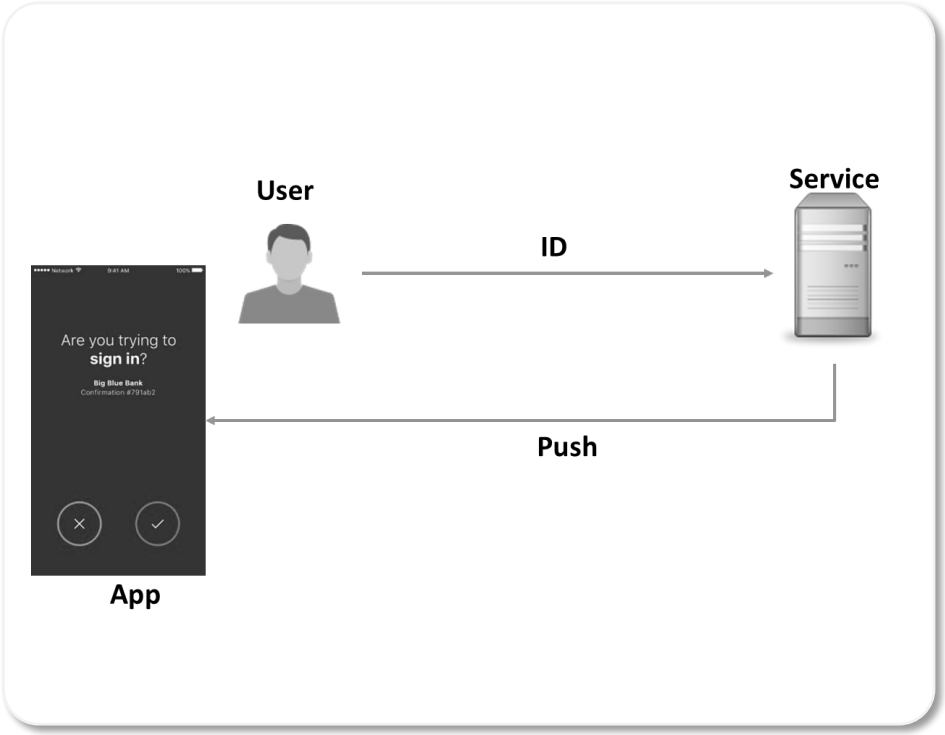
보안규정 대비 지켜지기 힘든 암호관리의 현실

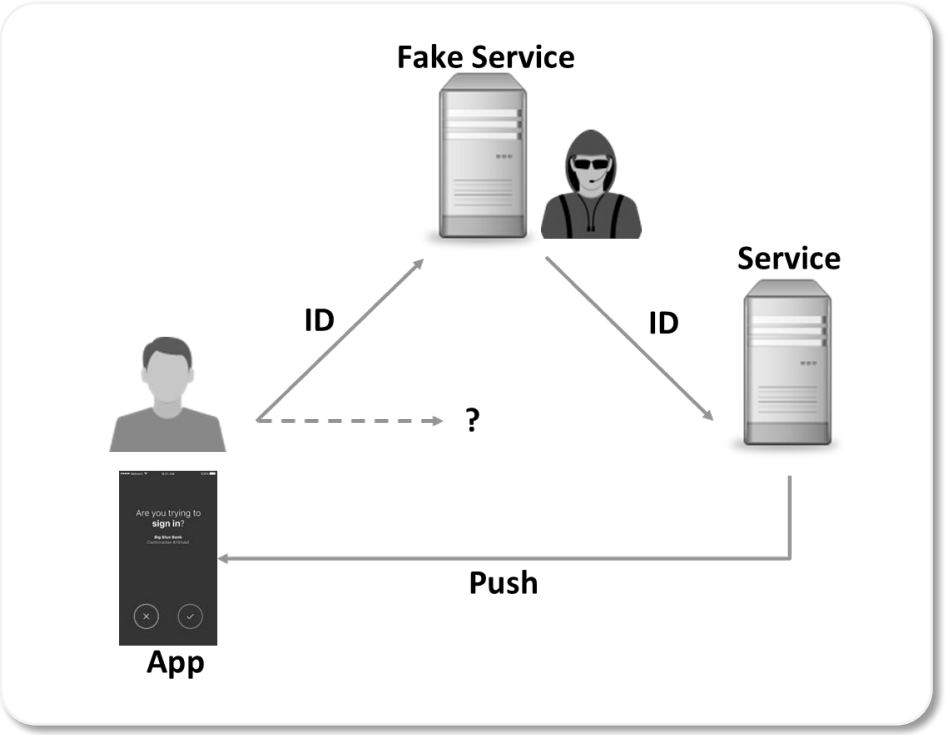
업무용 컴퓨터, 기업 서버, 다양한 비즈니스 웹서비스에는 지정한 사용자 이외에 아무나 접근할 수 없게 관리해야 하는 보안규정은 존재하지만, 아이디와 암호를 입력할 때 누군가가 엿볼 수 있고, 특정 주기 마다 암호를 변경하다 보면 책상 위에 적어 놓거나 기억하기 쉬운 값을 사용하게 됩니다. 또한 부득이한 상황에 동료에게 암호를 알려주다 보면 규정을 준수하기 조차 쉽지 않습니다. 만약 이런 상황에서 해당 시스템에서 보안사고라도 발생하게 되면 누가 사고를 일으켰는지 입증하기도 어렵습니다.



01 암호 관리 현황 및 문제점

사용자만 인증하는 인증기술의 한계





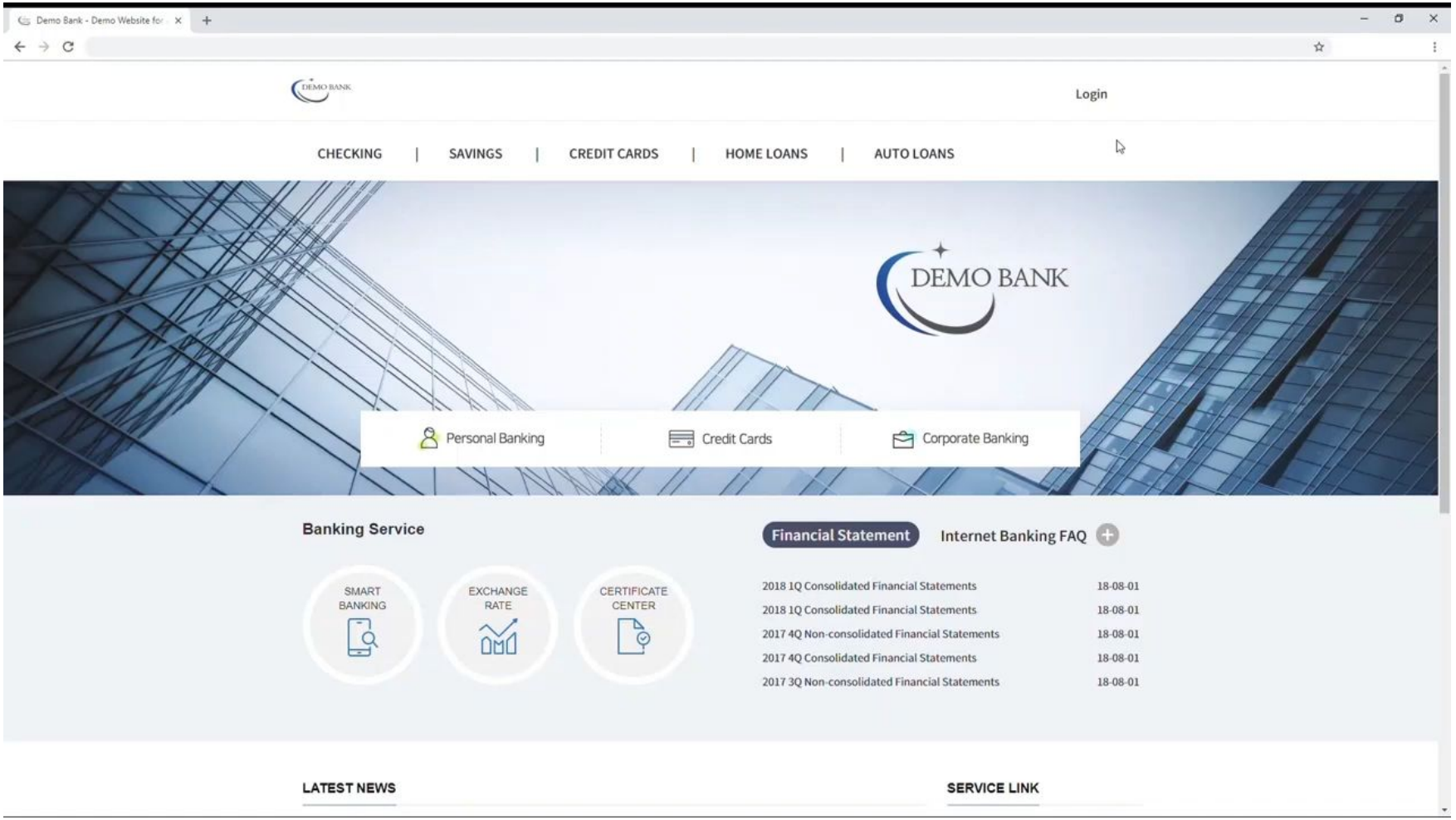
제품 소개

AutoPassword™

AutoPassword(자동 암호) 기술이란?

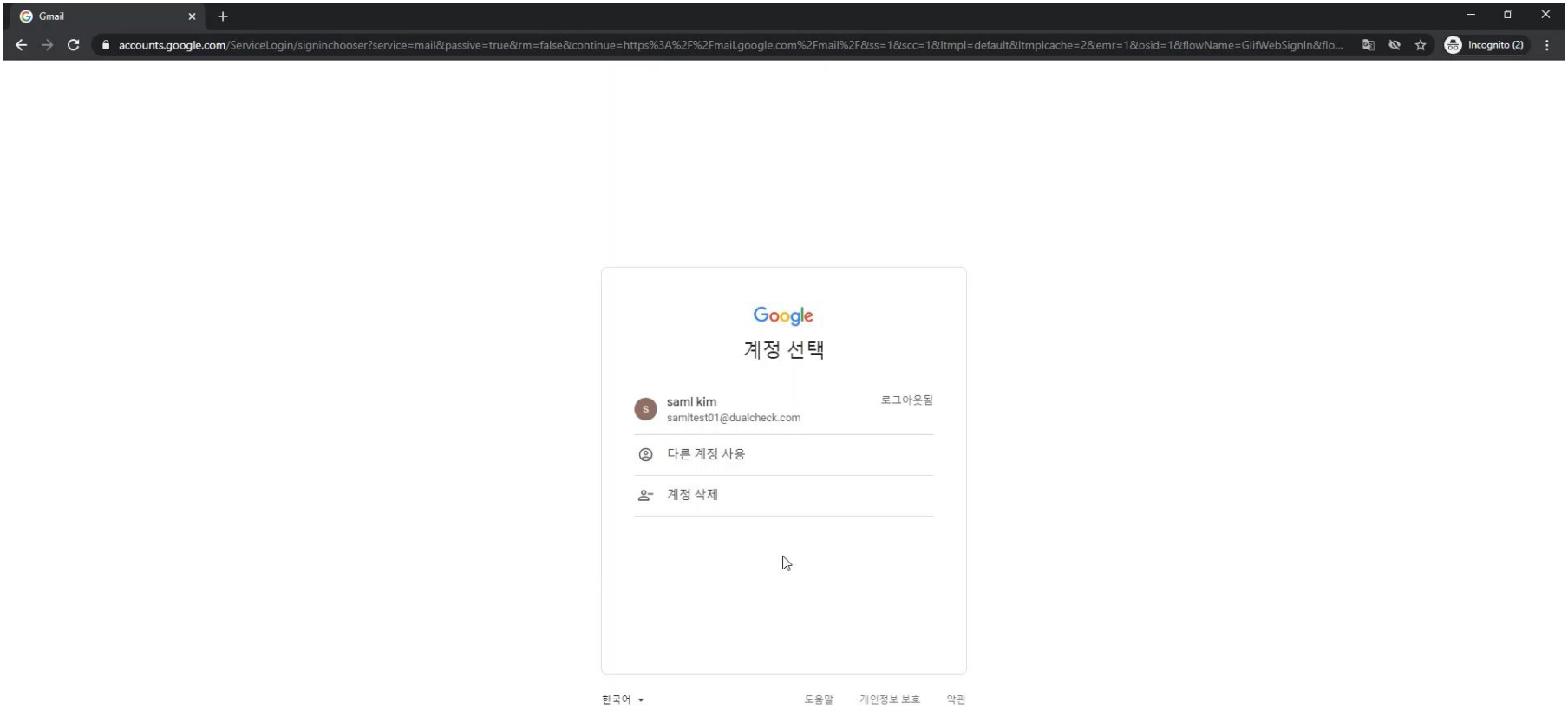
오토패스워드(AutoPassword)는 사용자가 온라인서비스나 업무시스템 또는 PC나 서버장치에 접속할 때 아이디만 입력하면 서비스쪽에서 일회용 비밀번호를 먼저 제시하고, 사용자는 스마트폰 앱을 통해 온라인서비스가 제시한 암호가 맞는지만 확인하면 되는 패스워드 대체 기술입니다. 오토패스워드는 서비스가 먼저 암호를 제시하기 때문에 접속한 웹사이트나 서비스, 장비가 가짜가 아닌지를 먼저 확인한 후에 이용할 수 있으면서, 사용자 입장에서는 패스워드를 외울 필요나 입력할 필요가 없어지기 때문에 사실상 패스워드 없이도 안전하게 온라인 서비스를 이용할 수 있게 됩니다. 따라서, 패스워드를 주기적으로 변경하거나 복잡한 규칙을 정해야 할 이유도 사라지게 됩니다.

오토패스워드를 이용한 웹사이트 로그인 시연



문서내 영상이 재생되지 않는 경우 유튜브 링크 클릭 https://youtu.be/zNMKlIyJ4uU

오토패스워드를 이용한 Google 서비스 로그인 시연

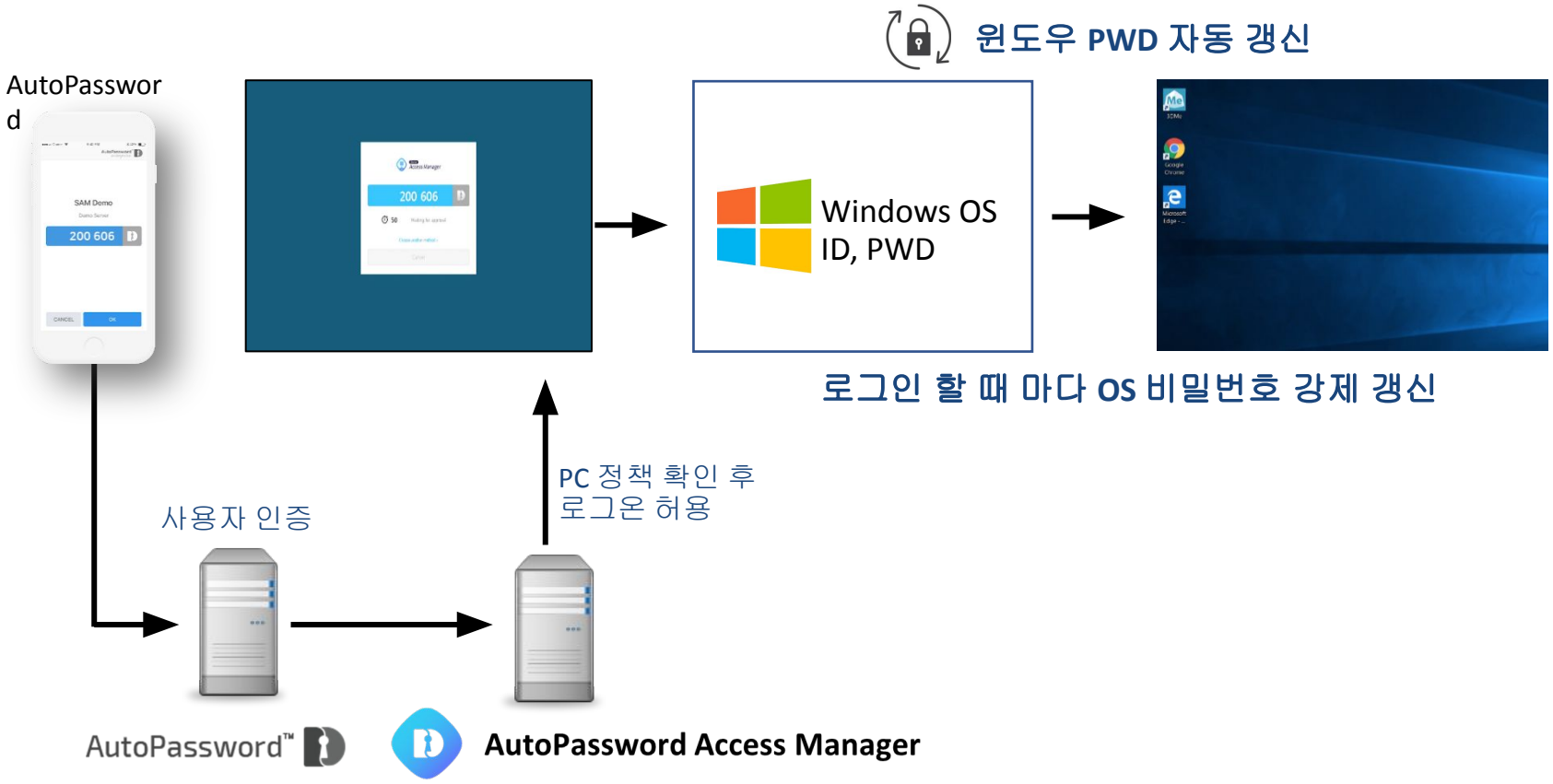


문서내 영상이 재생되지 않는 경우 유튜브 링크 클릭 https://youtu.be/l5H1C9gz7tg

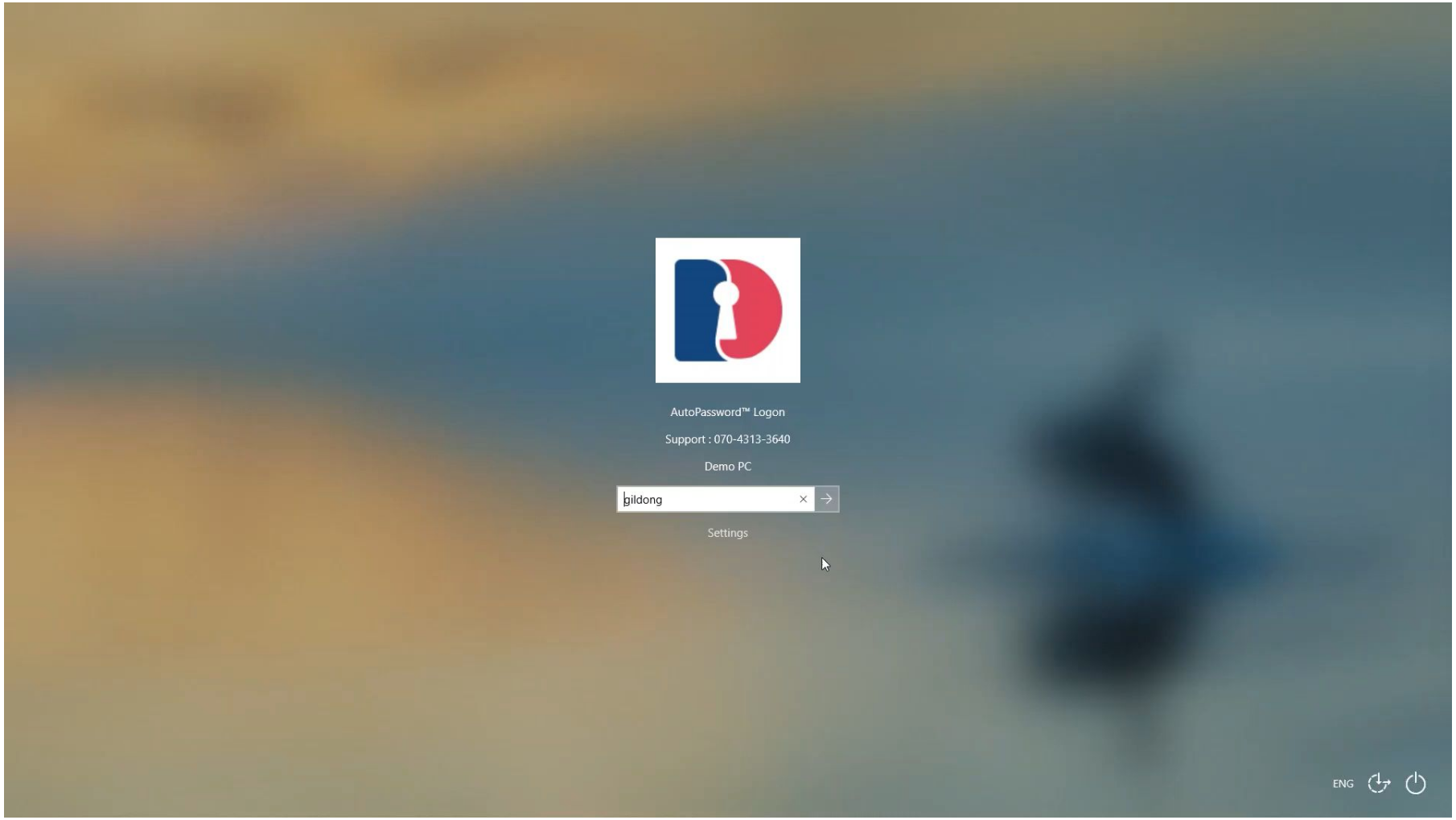

AutoPassword
Access Manager

자동 암호 기반의 단말기 접근 상호 인증

사용자가 암호를 입력하는 방식이 아니라 컴퓨터와 웹서비스가 스스로 자동 암호를 사용자에게 제시하고 사용자가 스마트폰에서 생성된 자동 암호와 같은지 확인하여 컴퓨터와 웹서비스를 사용할 수 있게 하는 모바일 기반 접근 관리 솔루션입니다. 사용자 암호 대신 자동 암호를 사용하여 사용자의 인증 값이 탈취되지 않는 보안성과 함께, 사용자가 로그온 할 때 마다 자동으로 컴퓨터와 웹서비스의 암호가 매번 변경되어 사용자는 암호 관리로 부터 해방됩니다.

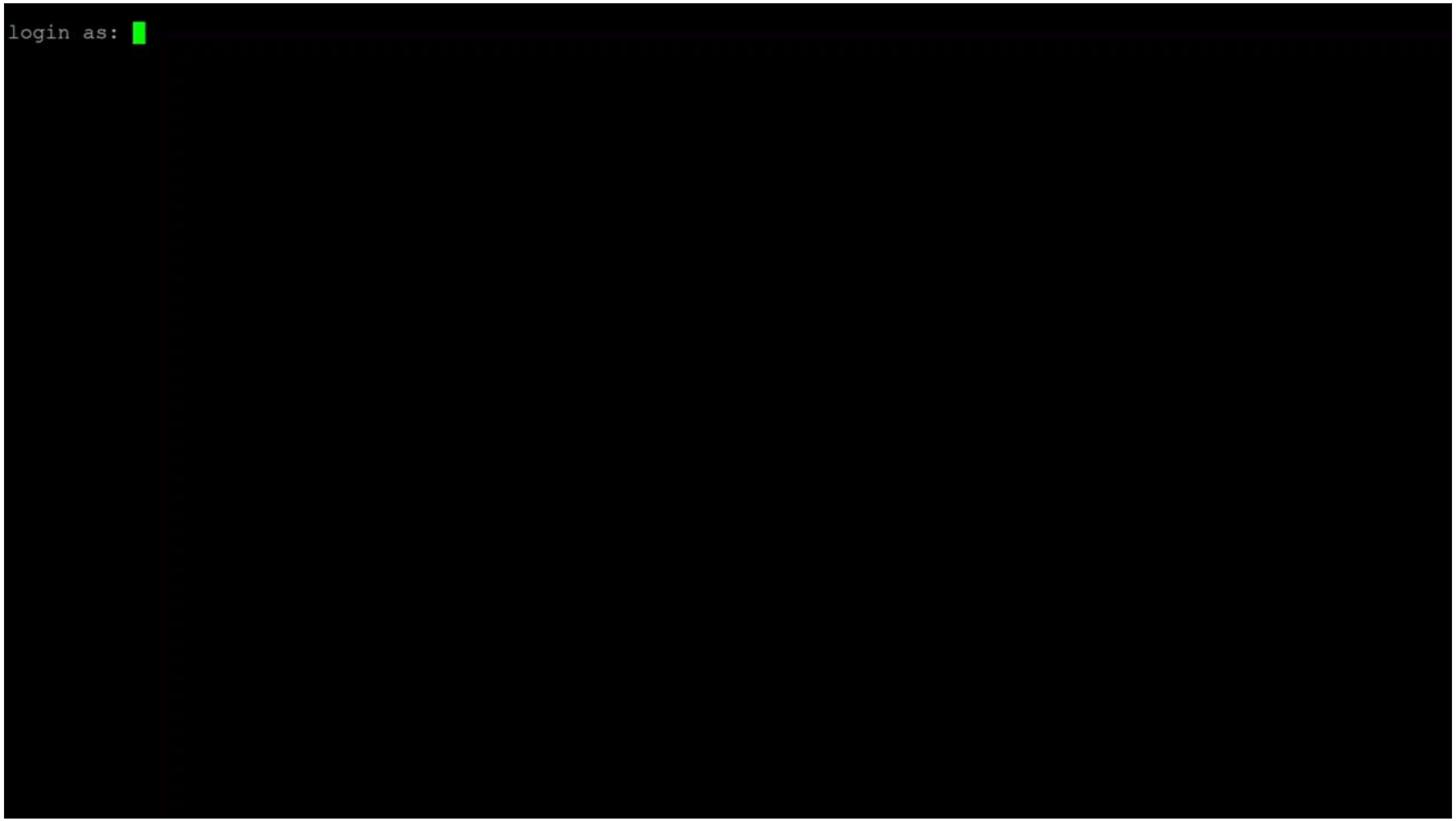


윈도우 PC 로그인 시연



문서내 영상이 재생되지 않는 경우 유튜브 링크 클릭 https://youtu.be/cjmjBDwgw00

리눅스 서버 로그인 시연

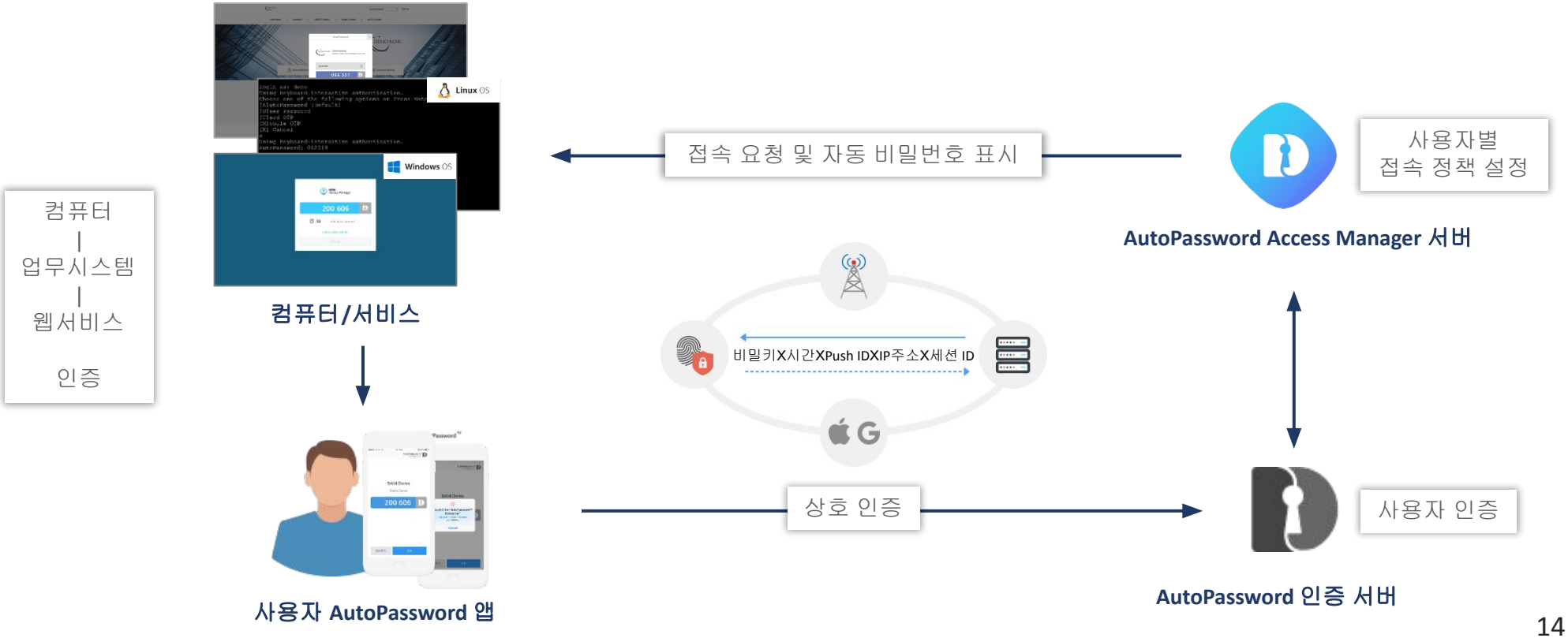


문서내 영상이 재생되지 않는 경우 유튜브 링크 클릭 https://youtu.be/FDt0i06otUI

제품 구조

접근 관리 서버와 연동된 컴퓨터 접근 권한 클라이언트 및 웹서비스용 API

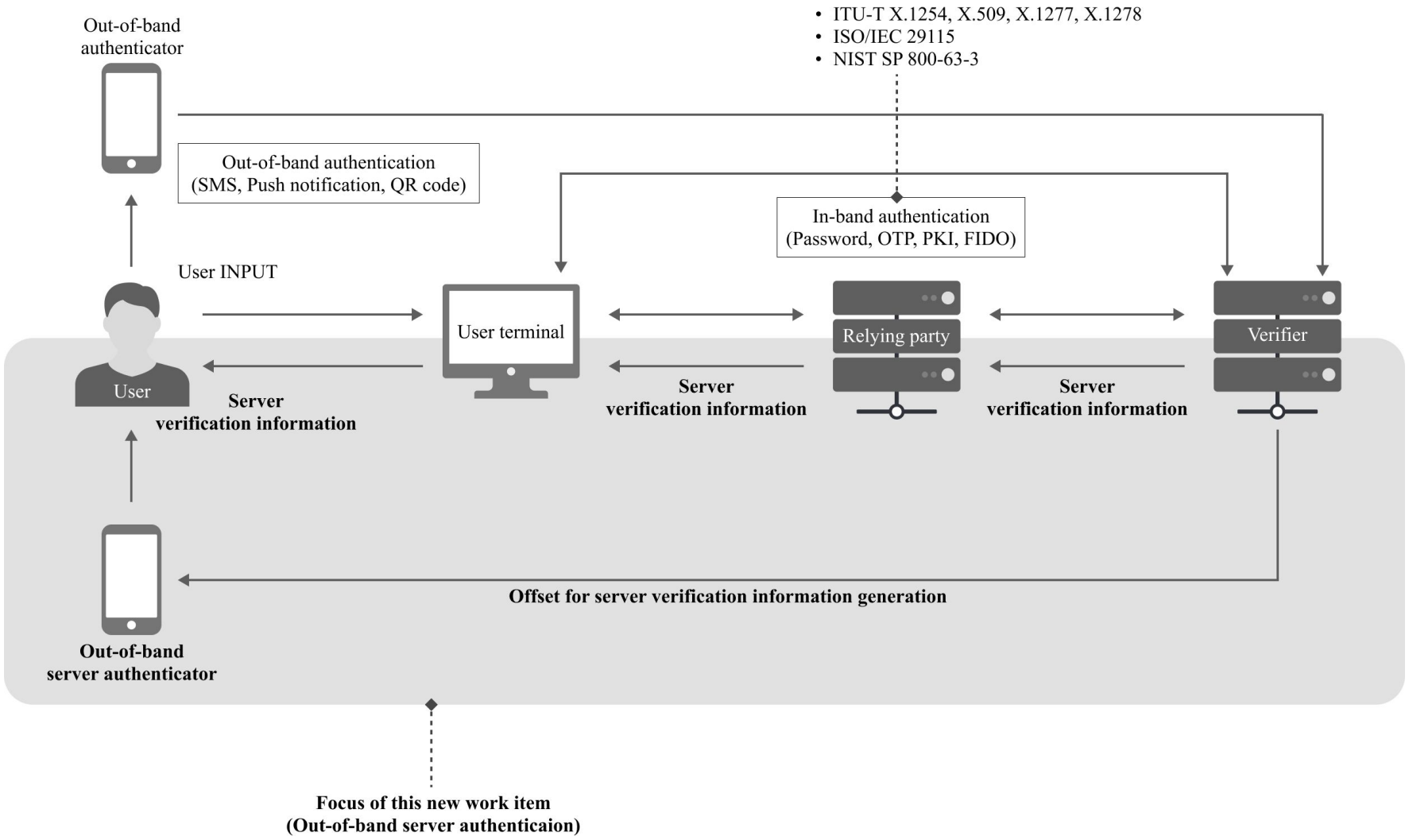
컴퓨터 접근 관리를 위해 사용자 컴퓨터에 설치되어 사용자 아이디와 암호를 관리하는 클라이언트 프로그램과 사용자와 접근가능 컴퓨터를 설정 할 수 있는 서버로 구성되어 있고, 웹서비스 접근 관리를 위해 RESTful API와 OAuth 2.0 방식으로 인증 부터 SSO 까지 가능한 API도 제공됩니다. 관리자가 클라이언트를 관리대상 컴퓨터에 설치한 후 서버의 관리 콘솔에서 사용자를 지정하면 지정된 사용자에 한하여 해당 컴퓨터를 사용할 수 있게 됩니다. 또한, 웹서비스는 적합한 API 연동을 통해 사용자 접근 관리가 가능합니다.



컴퓨터 및 웹서비스와 사용자간 상호 확인 후 로그인하는 상호 인증

사용자가 암호를 입력하는 것이 아니라 컴퓨터와 웹서비스가 스스로 자동 암호를 사용자에게 제시하고 사용자의 모바일을 통해서 이를 검증하기 때문에 더 이상 사용자 암호를 숙지하거나 변경할 필요가 없습니다. 컴퓨터와 웹서비스도 사용자의 폰과 사용자 본인을 확인한 후에 접근할 수 있게 제어합니다.

대역외 서비스 인증 기술 (Out-of-band server authentication)



제안사항

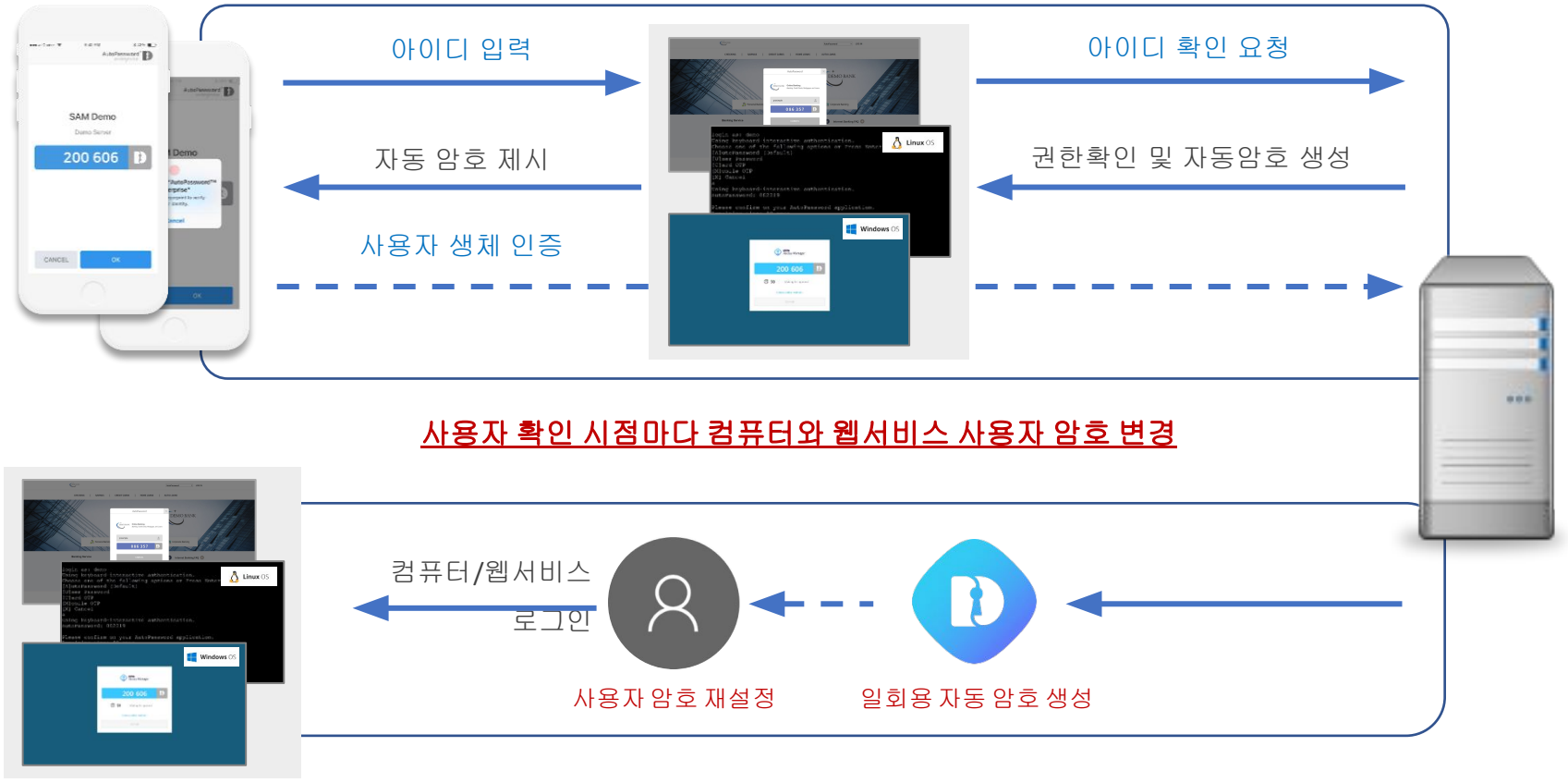
자동암호 기반 PC 및 업무시스템 통합 로그인 솔루션을 통해 편리성과 보안성을 동시에 강화하는 사용자 인증 체계 개선

추진배경 및 필요성	비밀번호 관리 어려움	• **업무시스템 증가로 인한 비밀번호 관리 부담 증가** - 여러 업무시스템별 비밀번호 숙지 및 변경 관리 부담 증가 • **비밀번호 유출 위험 증가** - 비밀번호 숙지의 어려움을 해소하고자 기재
	생체기반 인증 시대 도래	• **지식기반 인증으로 생체 기반 인증** - FIDO와 같은 생체정보 기반 인증의 보편화 • **단말 인증체계 강화와 업무 연속성 강화** - PC 로그인 인증을 기반으로 한 업무 연속성 강화
개선 방향	사용자 단말 인증체계 개선	• **PC 로그인 방식 개선** - 윈도우 비밀번호 기반에서 사용자 생체 기반 로그인 개선 • **모바일 FIDO 생체인증** - 사용자의 스마트폰 (안드로이드, iOS)을 지원
	PC로그인 기반 통합로그인 구축	• **윈도우 로그인 이후 업무시스템 자동 로그인** - 윈도우 로그인 이후 인증된 사용자 정보로 후속 시스템 자동 로그인 • **추후 유사 업무시스템 로그인 연동 확장 가능** - PC에서 사용되는 유사 프로그램에 대한 자동 로그인 지원

- ✔ 첫째, FIDO인증을 획득한 모바일 생체 인증 기술 적용
- ✔ 둘째, 자동 암호 PC 로그인 및 OS 비밀번호 자동 변경
- ✔ 셋째, 업무 PC 로그인 후, 업무 프로그램 자동 로그인
- ✔ 넷째, 사용자별 단말 및 업무용 어플리케이션 접근 관리

사용자 확인 시점 마다 자동으로 컴퓨터의 사용자 암호 변경

클라이언트 프로그램이 설치된 컴퓨터와 API가 연동된 웹서비스는 자동 암호를 생성하여 사용자에게 제시할 뿐만 아니라, 사용자가 자동 암호를 확인하는 과정에서 사용자 암호까지 변경합니다. 컴퓨터가 내부적으로 사용하는 사용자 암호와 웹서비스의 사용자 암호는 정책에 맞는 복잡한 임의의 값으로 설정되고, 사용자는 이를 숙지하거나 외울 필요 없이 컴퓨터와 웹서비스에서 제시하는 자동 암호가 스마트폰에 설치된 인증 앱에서 생성한 자동 암호와 같은 지 확인만 하면 됩니다.



FIDO (Fast Identity Online) Certification을 획득한 모바일 생체인증 시스템

- 일반 OTP(One Time Password)와는 차별화된 FIDO 기반 상호인증 기술
- 사용자의 스마트폰(Android, iOS)을 통한 안전한 역외 인증 방식
- 상호인증기술과 FIDO기술 결합을 통합 2중 보안


Certification

In recognition of eSTORM Co., Ltd.'s achievement of FIDO® UAF Certification

Company: eSTORM Co., Ltd.
Product: eSTORM DualAuth FIDO® Authenticator
Specification: Universal Authentication Framework (UAF)
Specification Version: 1.0 (2014-12-09)
Implementation Class: Authenticator
AAID: 0014#B001
Operating System:
Policy Version: 1.3.3
Interoperability Date: N/A
Conformance Self-Validation Date: , 2018
Derivative: Yes
Source Certificate(s): UAF100020150520019

fido CERTIFIED UAF

Certificate No.
UAF100020180228002
Issued
February 28, 2018


Certification

In recognition of eSTORM Co., Ltd.'s achievement of FIDO® UAF Certification

Company: eSTORM Co., Ltd.
Product: eSTORM DualAuth FIDO® Server
Specification: Universal Authentication Framework (UAF)
Specification Version: 1.0 (2014-12-09)
Implementation Class: Server
Policy Version: 1.3.3
Interoperability Date: N/A
Conformance Self-Validation Date: April 6, 2018
Derivative: Yes
Source Certificate(s): UAF100020150520021

fido CERTIFIED UAF

Certificate No.
UAF100020180410003
Issued
April 10, 2018


Certification

In recognition of eSTORM Co., Ltd.'s achievement of FIDO® UAF Certification

Company: eSTORM Co., Ltd.
Product: eSTORM DualAuth FIDO® Client
Specification: Universal Authentication Framework (UAF)
Specification Version: 1.0 (2014-12-09)
Implementation Class: Client
Policy Version: 1.3.3
Interoperability Date: N/A
Conformance Self-Validation Date: January 31, 2018
Derivative: Yes
Source Certificate(s): UAF100020150520020

fido CERTIFIED UAF

Certificate No.
UAF100020180208001
Issued
February 8, 2018


Certification

In recognition of eSTORM Co., Ltd.'s achievement of FIDO® UAF Certification

Company: eSTORM Co., Ltd.
Product: eSTORM DualAuth FIDO® Client/Authenticator Suite for iOS
Specification: Universal Authentication Framework (UAF)
Specification Version: 1.0 (2014-12-09)
Implementation Class: Client/Authenticator Combination
AAID: 0014#BA01
Operating System: iOS
Policy Version: 1.3.3
Interoperability Date: N/A
Conformance Self-Validation Date: April 3, 2018
Derivative: Yes
Source Certificate(s): UAF100020160323007

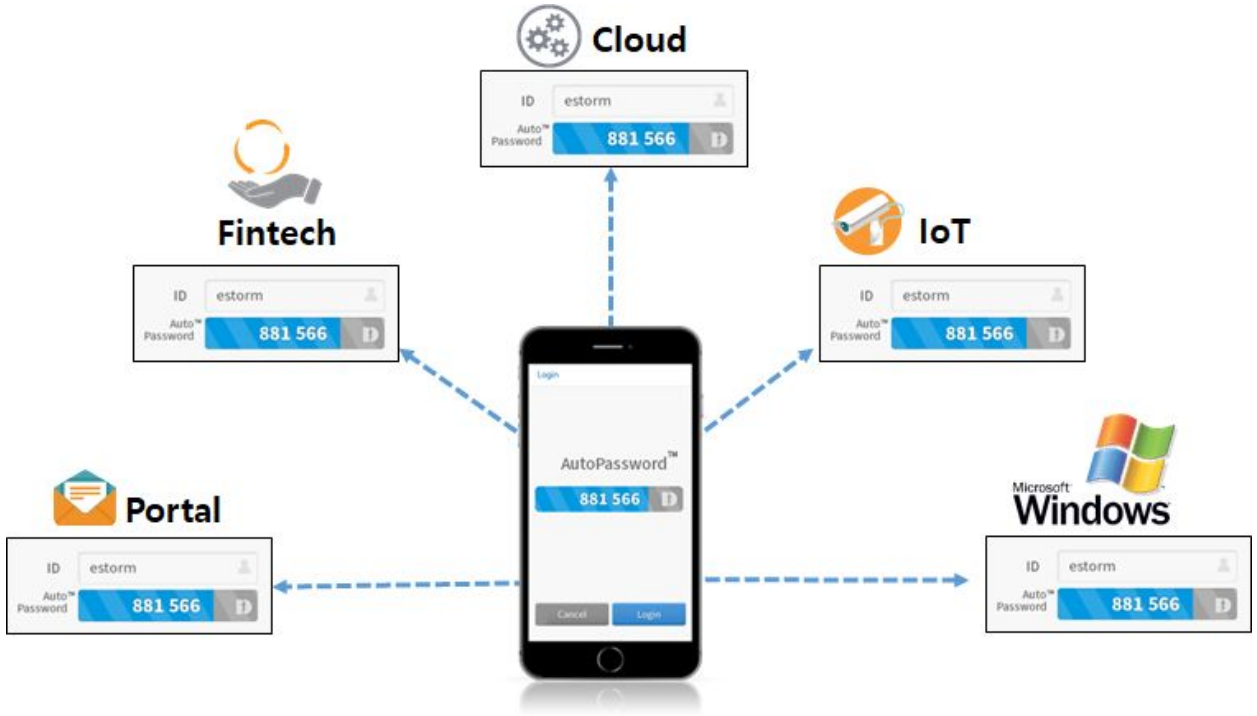
fido CERTIFIED UAF

Certificate No.
UAF100020180410001
Issued
April 10, 2018

크로스오버 FIDO 인증 기술

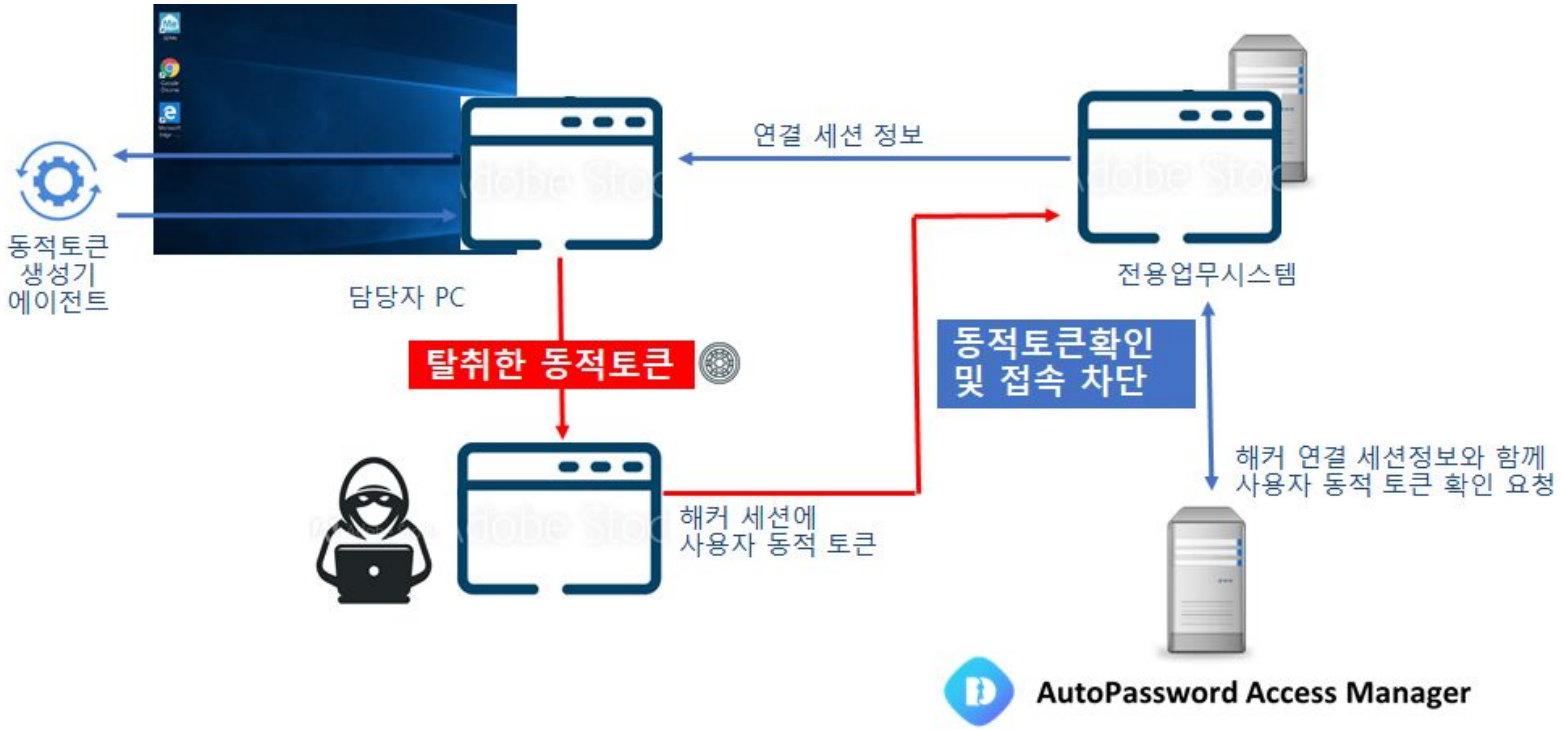
기관 및 기업에서는 오토패스워드를 도입하는 것만으로도 PC, 서버, 공공 웹서비스를 안전하게 보호하면서 사용할 수 있게 됩니다. 사용자는 오토패스워드를 통해 사용자의 인증 값이 탈취되지 않는 보안성과 함께, 사용자가 로그온 할 때 마다 자동으로 컴퓨터와 웹서비스의 사용자 암호가 매번 변경되기 때문에 사용자는 사용자 암호 관리를 할 필요가 없게 됩니다.

또한, PC나 서버의 접근관리 뿐만 아니라, 웹서비스 접근 관리에 사용될 수 있도록 RESTful API와 OAuth 2.0 방식으로 인증부터 SSO(Single Sign On) 까지 가능한 API를 제공하여 다양한 업무시스템에 싱글 인증체계를 확립할 수 있습니다.

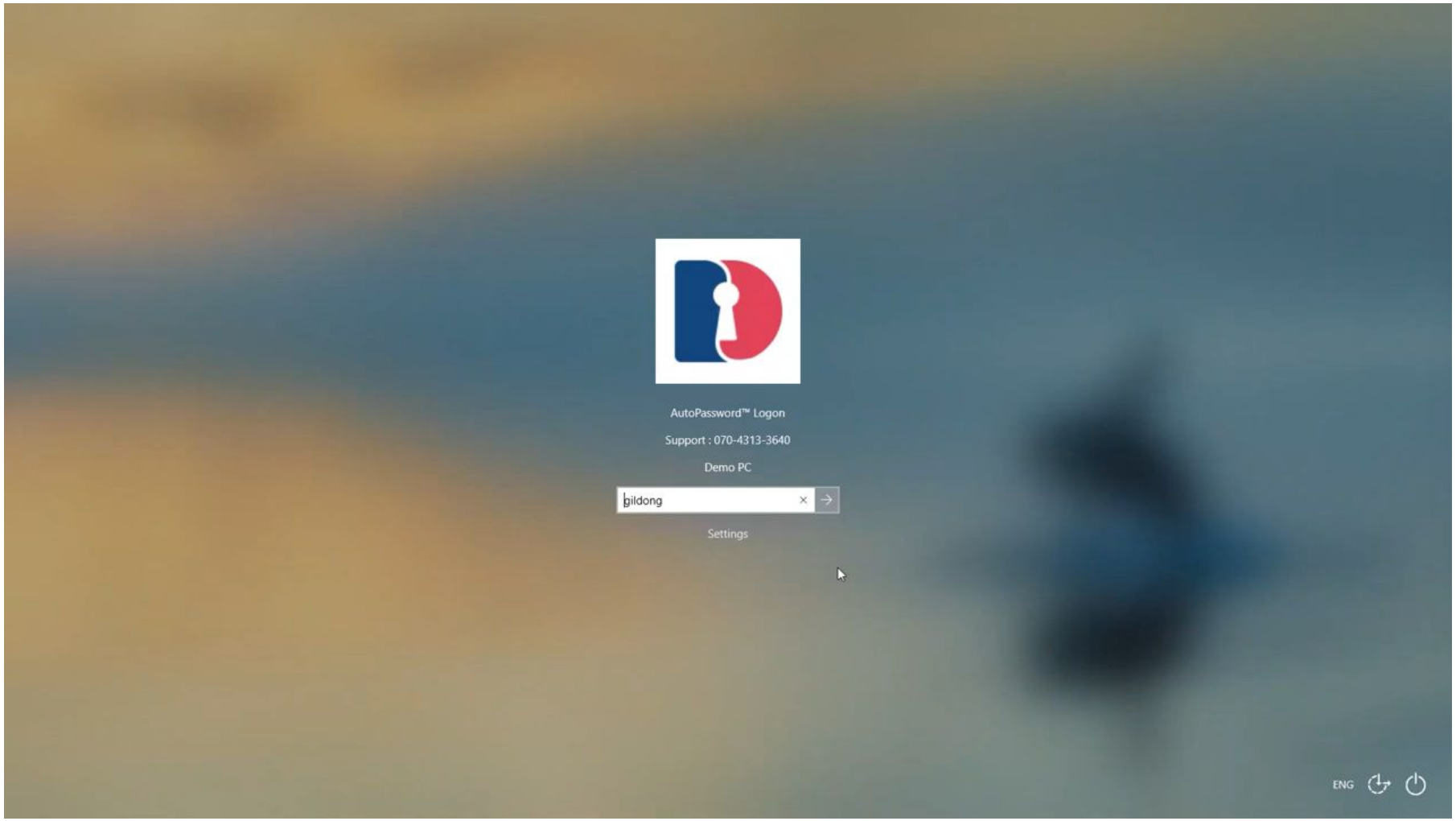


AutoPassword PCSSO 시스템을 통해 업무 프로그램 자동로그인 시스템 구축 (Option)

- 동적 토큰 방식으로 윈도우PC에 로그인한 인증값을 기반으로 업무시스템 자동로그인
- 역외인증 방식의 상호인증 기술을 통하여 사용자 토큰값이 탈취된 경우에는 접속 차단
- 관리자의 정책에 따라 AutoPassword 기반 자동 또는 반자동 로그인 적용



PC에서 업무프로그램 자동 로그인 시연



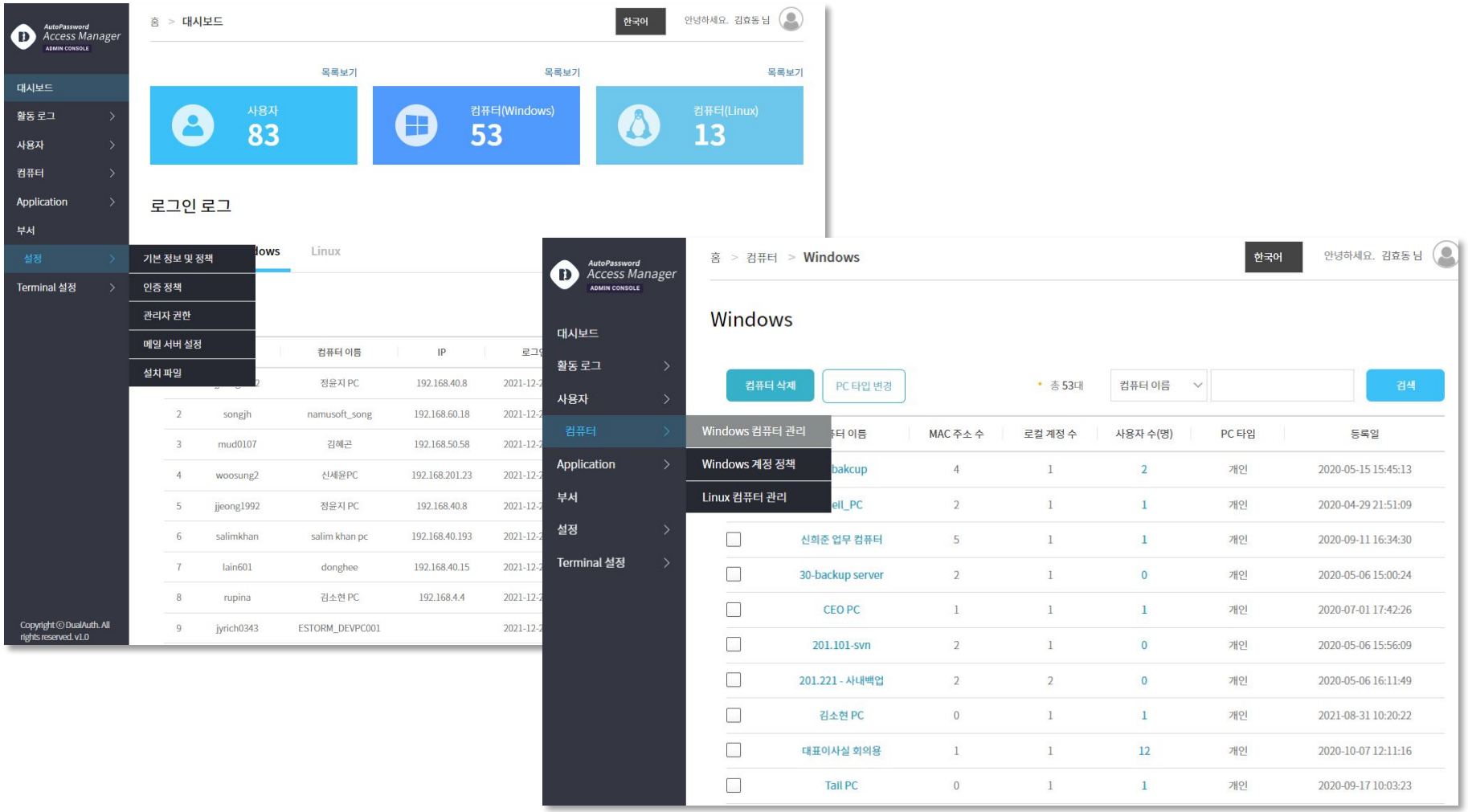
문서내 영상이 재생되지 않는 경우 유튜브 링크 클릭 https://youtu.be/l51h369QxXE

사용자별 PC 단말 및 업무시스템 접근 권한에 대한 관리를 통해 보안성 강화

- 사용자별 PC 및 어플리케이션 접근 대상 및 권한 설정
- 사용자별 PC 내 어플리케이션에 대한 자동 로그인 방식 개별 설정
- 사용자별 PC 및 업무시스템 이용 이력 등의 로그 관리
- 전사캠페인을 위한 바탕화면 설정 및 스크린세이버 설정

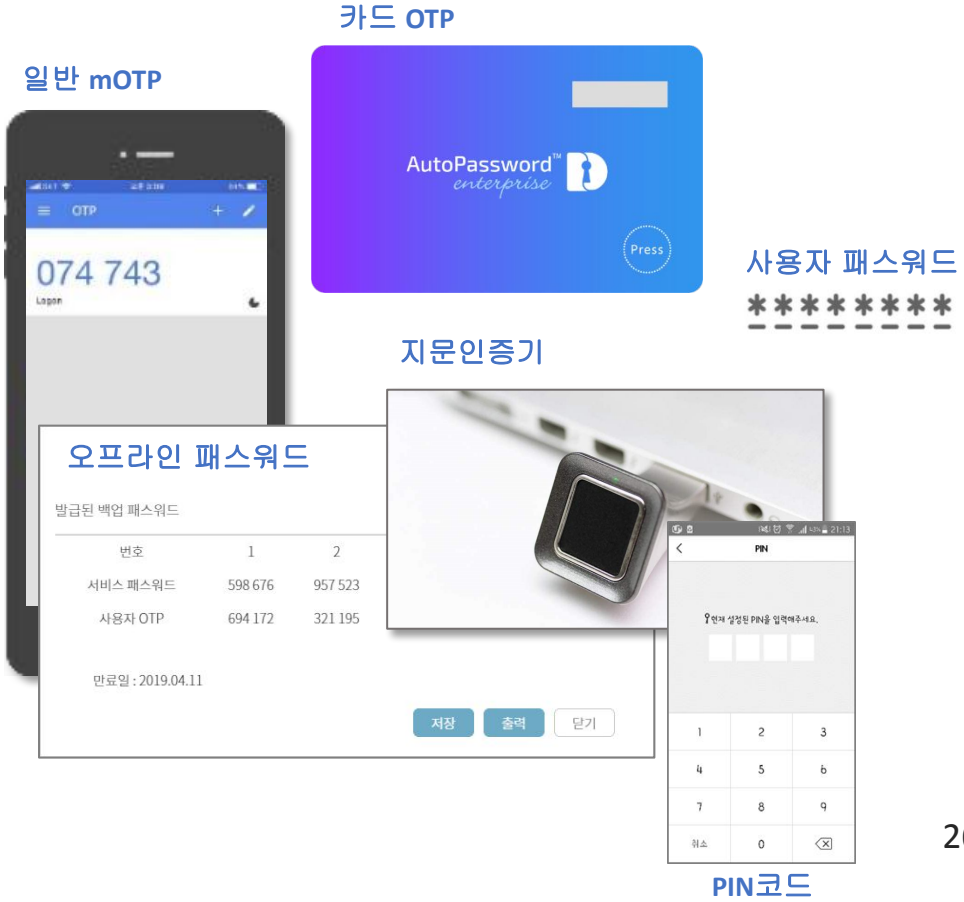
04 제안사항

주요 관리 화면



스마트폰 분실 및 인터넷 연결이 어려운 상황을 위한 대체 인증 수단 제공

스마트폰 분실 및 파손, 인증 앱 삭제 등과 같은 상황에서도 컴퓨터와 웹서비스 접근이 가능할 수 있도록 관리자는 OTP 카드를 발급해 주거나 백업 패스워드를 발급하여 출력물이나 이메일 등으로 사용자에게 제공할 수 있게 합니다. 또한 사전에 컴퓨터 오프라인 설정을 한 경우 컴퓨터의 인터넷 연결이 불가능한 오프라인 상태에서도 컴퓨터를 사용할 수 있도록 시간 동기화 모바일 OTP를 등록하여 사용할 수 있습니다.



제품 기술력

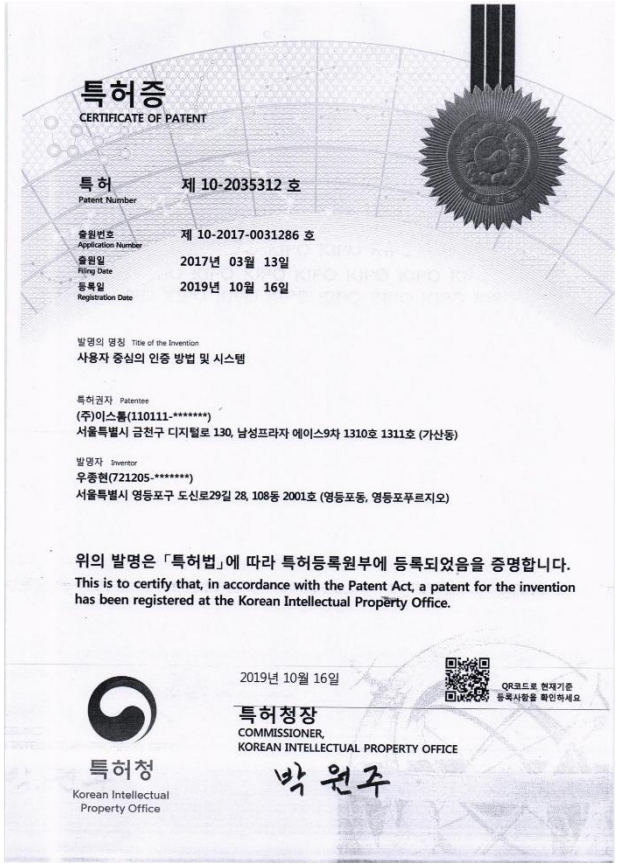
패스워드의 패러다임 전환

지난 60년간 모든 인증기술이 사용자만 확인하는 사용자 인증 기술 (비밀번호, OTP, PKI, 생체인증) 이었으나 **'AutoPassword'**는 사용자가 접속한 온라인 서비스가 진짜인지 가짜인지를 육안으로 직접 확인할 수 있게 하는 서비스 인증 개념을 기존 사용자 인증기술에 추가한 유일한 상호인증 기술입니다.

AutoPassword™

AutoPassword는 사용자가 원격지 서비스에 접속하였을 때, ① 사용자가 온라인 서비스에 ID를 입력하면 ② 온라인 서비스가 먼저 사용자에게 일회용 자동 비밀번호를 제시하고 ③ 사용자는 온라인 서비스가 제출한 일회용 자동 비밀번호가 맞는지 자신의 스마트폰에서 생성된 일회용 자동 비밀번호와 비교하여 일치하면(온라인 서비스의 진위여부 확인), ④ 자신의 생체정보(지문, 안면 등)를 스마트폰에 입력하여 온라인 서비스에 사용자를 인증시키는 상호인증 기술입니다.

대한민국, 미국, 일본 3개국 특허 등록 완료



특허증
CERTIFICATE OF PATENT

특허 Patent Number 제 10-2035312 호
출원번호 Application Number 제 10-2017-0031286 호
출원일 Filing Date 2017년 03월 13일
등록일 Registration Date 2019년 10월 16일

발명의 명칭 Title of the Invention
사용자 중심의 인증 방법 및 시스템

특허권자 Patentee
(주)이스톰(110111-*******)
서울특별시 금천구 디지털로 130, 남성프라자 에이스9차 1310호 1311호 (가산동)

발명자 Inventor
우종현(721205-*******)
서울특별시 영등포구 도신로29길 28, 108동 2001호 (영등포동, 영등포푸르지오)

위의 발명은 「특허법」에 따라 특허등록원부에 등록되었음을 증명합니다.
This is to certify that, in accordance with the Patent Act, a patent for the invention has been registered at the Korean Intellectual Property Office.

2019년 10월 16일

특허청장
COMMISSIONER,
KOREAN INTELLECTUAL PROPERTY OFFICE
박 원주

특허청
Korean Intellectual Property Office

2019년 10월 등록

特許証
(CERTIFICATE OF PATENT)

特許第6799142号
(PATENT NUMBER)

発明の名称 (TITLE OF THE INVENTION) 認証方法及びシステム

特許権者 (PATENTEE) 大韓民国，０８５８９ ソウル，グムチョン－グ，ディジタルーロ，１３０，１３１０ホ １３１１ホ
国籍・地域 大韓民国
イーストーム カンパニー，リミテッド

発明者 (INVENTOR) ウ，ジョン ヒョン

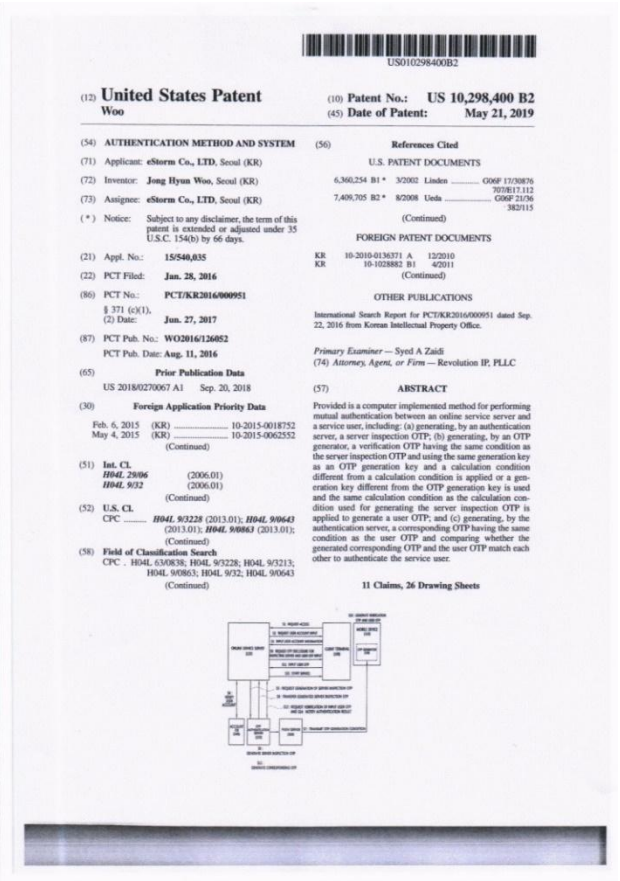
出願番号 (APPLICATION NUMBER) 特願２０１９－５０７０５７
出願日 (FILING DATE) 平成２９年 ３月２８日(March 28, 2017)
登録日 (REGISTRATION DATE) 令和 ２年１１月２４日(November 24, 2020)

この発明は、特許するものと確定し、特許原簿に登録されたことを証する。
(THIS IS TO CERTIFY THAT THE PATENT IS REGISTERED ON THE REGISTER OF THE JAPAN PATENT OFFICE.)

令和 ２年１１月２４日(November 24, 2020)

特許庁長官
(COMMISSIONER, JAPAN PATENT OFFICE)
糟谷敏秀

2020년 11월 등록



US010298400B2

(12) United States Patent
Woo

(10) Patent No.: US 10,298,400 B2
(45) Date of Patent: May 21, 2019

(54) AUTHENTICATION METHOD AND SYSTEM

(71) Applicant: eStorm Co., LTD, Seoul (KR)
(72) Inventor: Jong Hyun Woo, Seoul (KR)
(73) Assignee: eStorm Co., LTD, Seoul (KR)
(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 66 days.

(21) Appl. No.: 15/540,035
(22) PCT Filed: Jan. 28, 2016
(86) PCT No.: PCT/KR2016/000951
§ 371 (c)(1),
(2) Date: Jun. 27, 2017
(87) PCT Pub. No.: WO2016/126052
PCT Pub. Date: Aug. 11, 2016

(65) Prior Publication Data
US 2018/0270067 A1 Sep. 20, 2018

(30) Foreign Application Priority Data
Feb. 6, 2015 (KR) 10-2015-0018752
May 4, 2015 (KR) 10-2015-0062552
(Continued)

(51) Int. Cl.
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
(Continued)

(52) U.S. Cl.
CPC *H04L 9/3228* (2013.01); *H04L 9/0643* (2013.01); *H04L 9/0863* (2013.01);
(Continued)

(58) Field of Classification Search
CPC . H04L 63/0838; H04L 9/3228; H04L 9/3213; H04L 9/0863; H04L 9/32; H04L 9/0643
(Continued)

(56) References Cited
U.S. PATENT DOCUMENTS
6,360,254 B1 * 3/2002 Linden G06F 17/30876 709/217
7,409,705 B2 * 8/2008 Ueda G06F 21/36 382/115
(Continued)
FOREIGN PATENT DOCUMENTS
KR 10-2010-0136371 A 12/2010
KR 10-1028882 B1 4/2011
(Continued)
OTHER PUBLICATIONS
International Search Report for PCT/KR2016/000951 dated Sep. 22, 2016 from Korean Intellectual Property Office.

Primary Examiner — Syed A Zaidi
(74) *Attorney, Agent, or Firm* — Revolution IP, PLLC

(57) ABSTRACT
Provided is a computer implemented method for performing mutual authentication between an online service server and a service user, including: (a) generating, by an authentication server, a server inspection OTP; (b) generating, by an OTP generator, a verification OTP having the same condition as the server inspection OTP and using the same generation key as an OTP generation key and a calculation condition different from a calculation condition is applied or a generation key different from the OTP generation key is used and the same calculation condition as the calculation condition used for generating the server inspection OTP is applied to generate a user OTP; and (c) generating, by the authentication server, a corresponding OTP having the same condition as the user OTP and comparing whether the generated corresponding OTP and the user OTP match each other to authenticate the service user.

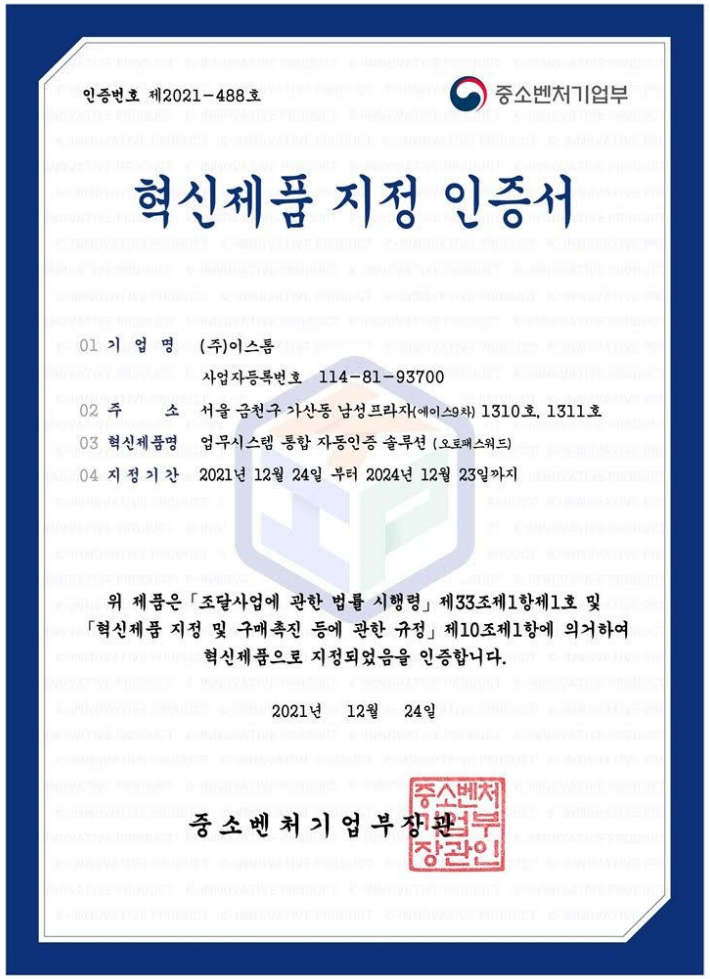
11 Claims, 26 Drawing Sheets

2019년 05월 등록

"사용자 중심의 인증 방법 및 시스템"

대한민국 혁신제품 지정

오토패스워드는 기술의 혁신성을 인정받아 2021년 12월 중소벤처기업부로부터 대한민국 혁신제품으로 지정되었습니다.



인증번호 제2021-488호

중소벤처기업부

혁신제품 지정 인증서

01 기 업 명 (주)이스롬
사업자등록번호 114-81-93700

02 주 소 서울 금천구 가산동 남성프라자(에이스9차) 1310호, 1311호

03 혁신제품명 업무시스템 통합 자동인증 솔루션 (오토패스워드)

04 지 정 기 간 2021년 12월 24일 부터 2024년 12월 23일까지

위 제품은 「조달사업에 관한 법률 시행령」 제33조제1항제1호 및
「혁신제품 지정 및 구매촉진 등에 관한 규정」 제10조제1항에 의거하여
혁신제품으로 지정되었음을 인증합니다.

2021년 12월 24일

중소벤처기업부장관

중소벤처기업부 장관인

[혁신제품 지정 인증서]

혁신제품

혁신제품으로 지정된 '오토패스워드'는 구매 목표제, 시범구매 사업, 수의계약 등이 가능한 혁신 조달 사업의 대상 제품입니다. 공공기관에서는 조달청 혁신조달 플랫폼인 혁신장터를 통해서도 솔루션을 구매할 수 있습니다.

[공공기관의 혁신제품 구매 혜택]

1. 수의계약 근거

혁신제품은 수의계약을 통해 구매할 수 있음

* 법적 근거: 「국가계약법 시행령」 제26조 제1항 제5호 사목
「지방계약법 시행령」 제25조 제1항 제8호 다 · 자목

2. 구매 면책

혁신제품을 구매한 수요기관의 구매책임자는 고의나 중대한 과실이 입증되지 아니하면 그 제품의 구매로 생긴 손실에 대하여 책임을 지지 않음

* 법적 근거: 「조달사업에 관한 법률」 제27조 제4항

3. 기관평가 반영

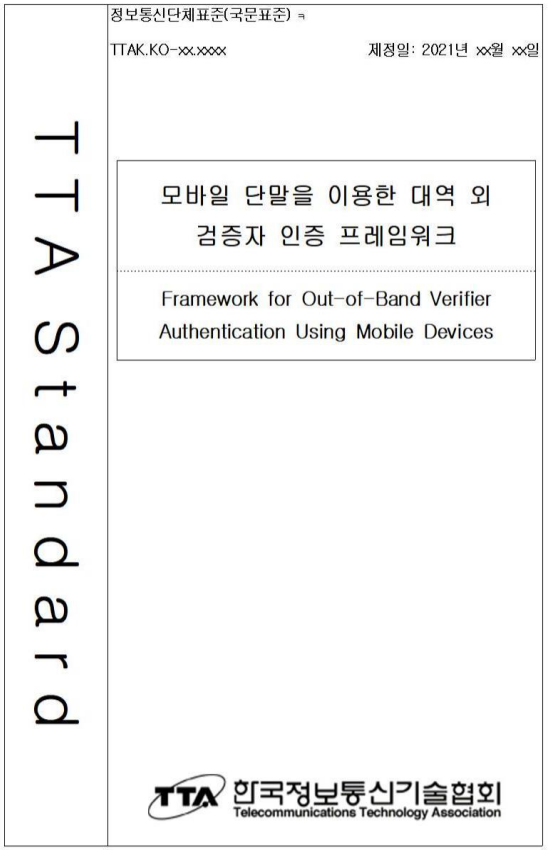
기관별 총 물품구매액의 1.6%(지자체 0.8%)를 혁신제품 구매에 활용하고 실제 구매실적을 기관평가에 반영

* 혁신구매액 인정범위: 혁신제품 구매액 + 기타혁신구매(경진대회 · 공모사업 상금 및 공공부문 R&D 결과물구매액 등)
* 정부혁신평가(중앙부처), 지방자치단체 합동평가(지자체), 공기업 및 준정부기관 경영평가, 지방공기업 경영평가
* 평가항목 및 지표, 측정기준 등 세부사항은 기관별 평가계획 참조

국내 및 국제 기술 표준화 진행중 (ITU-T 국제 표준 기구에 국가대표 기술로 제출)

보유한 특허를 기반으로 국내 기술 표준화 기구인 TTA PG502에 2021년 하반기 표준화 심의 대상 기술로 채택되었고, UN산하 ITU-T 국제표준기구에 대한민국의 국가 기고서로 2021년 7월 제출이 완료되었습니다.

(국내 표준은 2022년 상반기 표준등록 예정이며, ITU-T 국제표준은 2023년 하반기 등록 예정입니다)


정보통신단체표준(국문표준)

TTAK.KO-xx.xxxx 제정일: 2021년 xx월 xx일

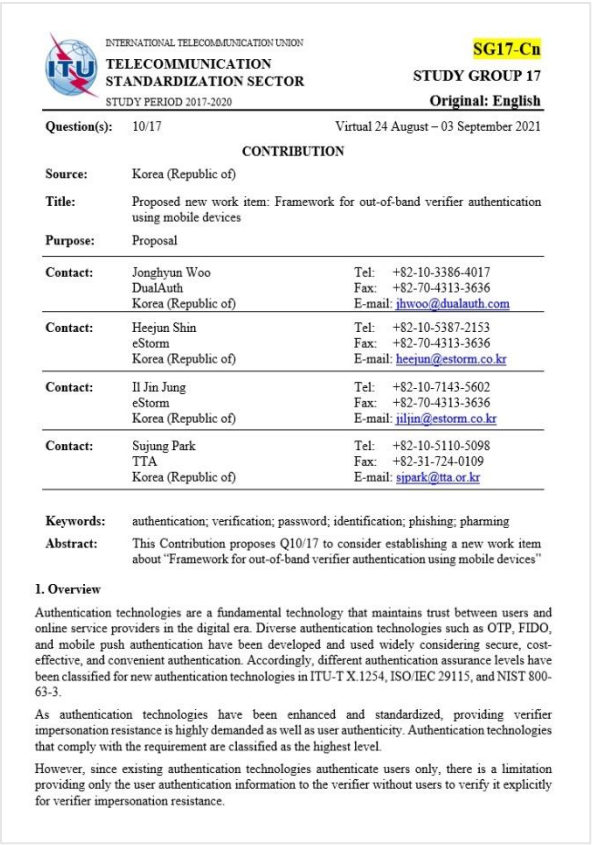
TTA Standard

모바일 단말을 이용한 대역 외 검증자 인증 프레임워크

Framework for Out-of-Band Verifier Authentication Using Mobile Devices

TTA 한국정보통신기술협회 Telecommunications Technology Association

[TTA기고서 표지]


INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

SG17-Cn

STUDY GROUP 17

Original: English

Question(s): 10/17 Virtual 24 August – 03 September 2021

CONTRIBUTION

Source: Korea (Republic of)

Title: Proposed new work item: Framework for out-of-band verifier authentication using mobile devices

Purpose: Proposal

Contact: Jonghyun Woo, DualAuth, Korea (Republic of) — Tel: +82-10-3386-4017, Fax: +82-70-4313-3636, E-mail: jhwoo@dualauth.com

Contact: Heejun Shin, eStorm, Korea (Republic of) — Tel: +82-10-5387-2153, Fax: +82-70-4313-3636, E-mail: heejun@estorm.co.kr

Contact: Il Jin Jung, eStorm, Korea (Republic of) — Tel: +82-10-7143-5602, Fax: +82-70-4313-3636, E-mail: iiljin@estorm.co.kr

Contact: Sujung Park, TTA, Korea (Republic of) — Tel: +82-10-5110-5098, Fax: +82-31-724-0109, E-mail: sjpark@tta.or.kr

Keywords: authentication; verification; password; identification; phishing; pharming

Abstract: This Contribution proposes Q10/17 to consider establishing a new work item about "Framework for out-of-band verifier authentication using mobile devices"

1. Overview

Authentication technologies are a fundamental technology that maintains trust between users and online service providers in the digital era. Diverse authentication technologies such as OTP, FIDO, and mobile push authentication have been developed and used widely considering secure, cost-effective, and convenient authentication. Accordingly, different authentication assurance levels have been classified for new authentication technologies in ITU-T X.1254, ISO/IEC 29115, and NIST 800-63-3.

As authentication technologies have been enhanced and standardized, providing verifier impersonation resistance is highly demanded as well as user authenticity. Authentication technologies that comply with the requirement are classified as the highest level.

However, since existing authentication technologies authenticate users only, there is a limitation providing only the user authentication information to the verifier without users to verify it explicitly for verifier impersonation resistance.

[ITU기고서 표지]

검증된 기술력

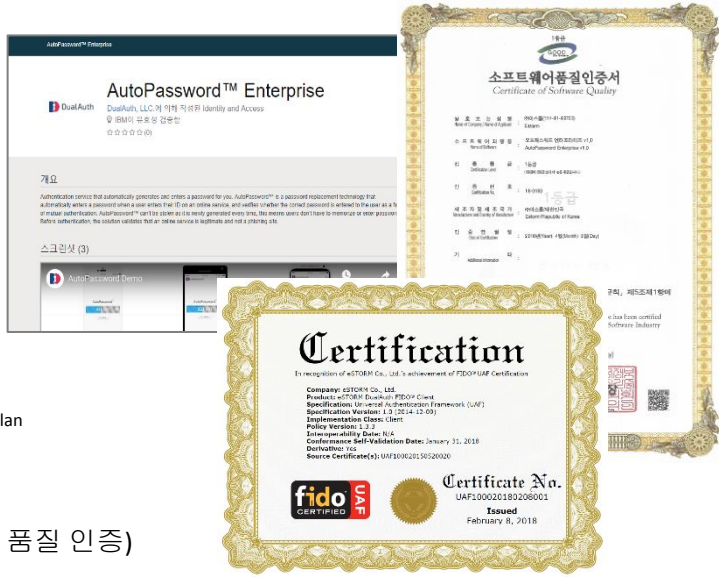
□ 특허 등록된 비밀번호 생성 알고리즘

AutoPassword의 인증 기술은 대한민국 및 미국에서 특허가 등록 완료되었습니다.

- 대한민국 특허 : 등록번호 제10-1513694호, 제10-1570314호, 제10-1570317호
- 미국 특허 : 등록번호 10,003,595
- 일본 특허 : 등록번호 6799142

□ 국내외에서 인정받은 기술력

- 대한민국 인터넷 대상 – 미래창조과학부 장관상 수상
- 한국인터넷진흥원 '핀테크 보안인증센터' – 인증분야 보안플랫폼 서비스 채택
- 핀테크 기술 경연대회 – 미국 뉴욕 피노베이트 (Finovate) 본선, 홍콩 피노베이트 아시아 본선 진출
- 영국 런던 '사이버 보안 및 사기 방지 (Anti-Fraud) 핀테크 어워드' TOP 5
- 일본 도쿄 – NTT Data 혁신 대회(Innovation Competition) 최종 라운드 진출



- 가트너 (Gartner) 리포트 – "균형이 잘 잡힌 (Well-Balanced) 인증 방법"으로 지목 [Push, Bio, FIDO]
  : 2017년 7월 "Don't Waste Time and Energy Tinkering With Password ; Invest in More Robust Authentication Method or Other Compensating Controls", Ant Allan
- 지문 인식 기술 관련 – FIDO (Fast Identity Online) 인증 획득
- IBM 보안접속매니저(Identity & Access Management) 유효성 검사 통과 – IBM 시큐리티 파트너 등록
- 대한민국 GS(Good Software)인증 1등급 획득 (소프트웨어산업진흥법 제13조에 의거한 소프트웨어 품질 인증)

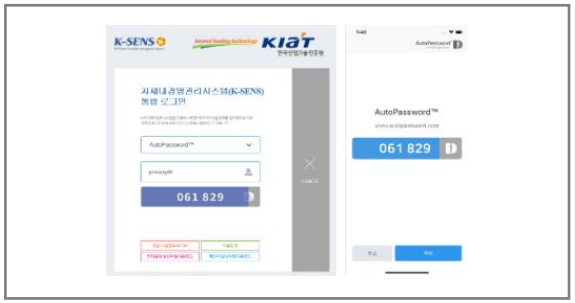
적용 분야

주요 적용 분야

사용성과 보안성을 겸비한 온/오프라인 상호인증 기술을 시장의 필요에 따라 다양한 상황에 적용되고 있으며, 크게 오토패스워드 엔터프라이즈와 오토패스워드 액세스 매니저 솔루션으로 제품을 공급하고 있습니다.

(1) 사용자 단말(PC) 접근보안

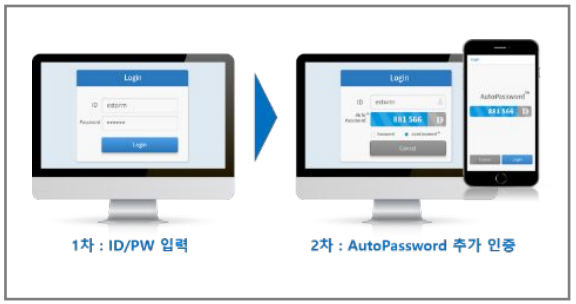
(2) 업무용 프로그램 접근보안



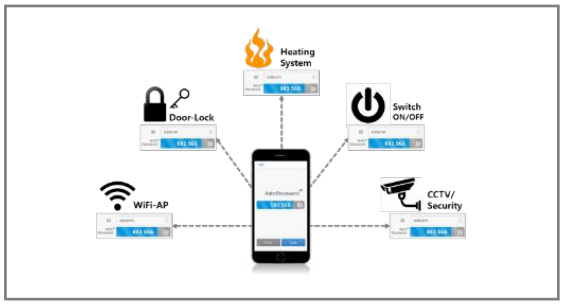
(3) 업무용 인프라 통합인증

(4) 서버 접근관리

(5) 2차인증(추가인증)



(6) IoT 기기의 통합접근관리



주요 도입 사례

청 와 대	청와대 – 대통령 비서실에서 도입하여 권한에 따른 노트북 PC 로그인 권한 제어로 안전한 PC 관리
통계청	국회도서관 – 통계청에서 도입하여 도서관내에 설치된 통계정보 열람 PC에 대한 로그인 권한 제어
우리은행	우리은행 – 지점을 포함한 전사 임직원의 PC 로그인 및 업무 포털 자동 로그인을 통한 사용자 인증체계 강화
HANSAE fashion worldwide	한세실업 – 사내 PC 자원의 권한에 따른 접근 제어 및 내부 업무 시스템 SSO와 연동하여 관리 일원화
KIAT	한국산업기술진흥원 – 임직원용 내부 업무시스템에 도입하여 내부망과 외부망에서의 개별적인 접근제어 운영
동두천시	동두천시청 – 시에서 운영중인 윈도우와 리눅스 서버의 접근 제어 및 OS비밀번호 주기적 자동 변경
CW 건설근로자공제회	건설근로자공제회 – 내부 시스템의 운영을 위한 서버 OS의 로그인 보안 강화
OPA 개인정보보호협회	개인정보보호협회 – 내부 업무망 접근 제어 및 공공기관 대상 OPA PASSWORD 공동 사업 진행
한국지능형사물인터넷협회 Korea Intelligent IoT Association	한국지능형사물인터넷협회 – 내부 업무시스템의 임직원 사용자 인증
브이피(주)	브이피 – ISP 인증 사업을 진행하는 BC카드 자회사로 BC카드 고객 대상 서비스 진행 및 공동 사업 진행
Do Dream 동두천	동두천 CCTV통합관제센터 – 열람 운영용 단말 장비의 접근 권한 부여 및 관리

주요 도입 효과

- ✔ 현재 연결하려는 서비스의 진위를 사용자가 먼저 확인하고 사용자 인증 값을 전달하는 상호 인증 방식의 자동 암호 사용을 통해 PC 및 업무시스템 접속시 사용자의 암호가 탈취될 염려가 없는 (피싱 및 파밍 원천 차단) 보안성 확보.

- ✔ 사용자가 암호를 입력하는 것이 아니라 PC나 업무시스템이 스스로 자동암호를 사용자에게 제시하고 사용자의 모바일을 통해 이를 자동으로 검증하기 때문에 사용자 패스워드를 입력하거나 외울 필요가 없어지는 사용 편리성 확보. (임직원 입장에서는 사실상 아이디만 입력하면 패스워드 없이 안전하게 컴퓨터 및 업무시스템을 이용)

- ✔ 사용자가 업무PC에 로그온 할 때 마다 자동으로 사용자 암호가 매번 변경되기 때문에 암호 관리로부터 해방되며, 비밀번호 주기적 변경 등 비밀번호 관리와 관련한 보안규정 자동 준수.

- ✔ 비밀 번호 관리에 대한 부담이 줄게 되어 IT 서비스 지원 부서의 비밀번호 관련 업무 최소화.

- ✔ 임직원별 PC와 업무시스템에 대한 접근 권한을 부여하고 본인 생체인증을 통해서 접속하게 되어 업무PC와 업무시스템 이용에 대한 사용자별, 시스템별 이력 관리 강화.

회사 소개

온라인 서비스부터 오프라인 신원확인까지 상대방을 먼저 확인 해주는 인증기술 전문기업

(주)이스톰은 1999년 설립되어 금융권 시스템 및 기업용 S/W와 문서 협업 솔루션을 지속적으로 개발해 왔으며, 현재는 보안 인증 솔루션 개발에 집중해 상호인증 및 페이먼트 기술을 개발/서비스 하고 있습니다. 특히, OTP를 이용한 서비스와 사용자간 상호 인증의 핵심기술을 개발해 런던, 뉴욕, 홍콩, 도쿄 등에서 열린 핀테크 경연대회에서 기술력을 인정받았으며, 한국과 미국, 일본에 기술 특허 등록을 완료하고 관련 제품을 정부기관 및 기업에 공급하면서 보안 인증 기술 전문 기업으로 발돋움하고 있습니다.

온/오프라인 상호인증 및 접근관리 솔루션 제공사

온라인 서비스 상호인증	단말기 접근 상호인증	시설물 이용 상호인증	신원확인 상호인증
AutoOTP™	AutoPassword™	AutoPassword ID Card	AutoPassword ID Card
AutoPassword™	AutoPassword Access Manager	AutoPassword ID Card Terminal	AutoPassword ID Card Reader

감사합니다

DualAuth

주요제품

- AutoPassword : 패스워드를 기억할 필요가 없는 모바일 자동 상호 인증 솔루션
- Enterprise : PC 및 서버의 로그인 보안 및 접근제어와 패스워드 자동 변경 솔루션
- AutoPassword Access Manager : 랜섬웨어를 완벽하게 예방하는 기업/기관용 파일 공유 디스크
- : 중요 파일을 완벽히 보호하는 스토리지 프로텍션 솔루션
- FilingBox Enterprise
- FilingBox MEGA

문의처

- 웹 사이트 : **www.filingcloud.co.kr**
- 이 메 일 : **support@autopassword.com**
- 전 화 : **02-6925-0290**
- 담 당 자 : **김효동 실장 02-6925-0290 (내선312)**

fido CERTIFIED UAF

TTA GS인증 1등급 | K-Innovative Product 혁신제품 | 조달청 나라장터 조달제품 등록

IBM Security