PASCON 2021
2021 공공 · 금융 · 기업 정보보안&개인정보보호 컨퍼런스

보안인증의 현재와 미래, 적용사례

옥타코 이재형, fimori@octatco.com

물리보안 & 사이버보안 디지털 아이덴티티 & 생체인증 전문

이재형

+10 years in Physical Security, Video Surveillance
(Moscow Sheremetyevo International Airport Terminal 3, Italy & Switzerland Railway, Dubai Internet City etc.)
+6 years in Cybersecurity, Digital Identity, Biometrics, FIDO
(The most FIDO2 Biometrics authenticator certified, MS FIDO2 Official Vendor, Samsung Insurance, Prudential etc.)
+5 biometric patent & +7 research paper on IRIS, Fingerprint & FIDO, Blockchain, PKI

2008년 산업자원부 선정 올해의 무역인
2010년 산업자원부 기술사업화 우수상
2020년 과기부 인공지능 엣지반도체 개발, 인공지능 생체인식 위,변조 방지 개발 책임
2020년 FIDO Korea Working Group 올해의 회원
2021년 FIDO Alliance Global Development Challenge 심사위원

SKT-IDQ-생체인증 벤처기업 옥타코, 양자보안 적용 지문인식 보안키 세계 첫 출시

IDQ), 생체인증 벤처기업 옥타코는 세계 최초로 양자난수생성

사진제공=SKT)

2021 Trends
Authentication & Identity Access

- MFA(다중인증) 인증 강화 추세
- Zero Trust 인증 모델 확대
- 생체인증 도입 확대
- MS, Apple, Google 등 Passwordless 이동 가속
- FIDO 기반인증 현재 전체 MFA 중 5%미만에서 2025년 25%로 성장 예상

2021 Trends

- Executive Order on Improving the Nation's Cybersecurity | The White House

2021.5.12일 Biden 행정부의 국가 사이버보안 강화 행정명령 발동

주요내용: MFA(다중인증), Zero Trust 모델, 표준화된 사건 보고를 의무화
미 연방정부, 연방기관, 주정부 및 관련 기관 해당

자료출처: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

fido ALLIANCE | simpler stronger authentication

Online Authentication Barometer

October 2021

What's the latest in consumer habits, trends and adoption of authentication technologies across the globe?

To find out, the FIDO Alliance conducted a survey of 10,000 consumers in the U.S., U.K., France, Germany, Australia, Singapore, Japan, South Korea, India and China.

자료출처: FIDO Alliance - Open Authentication Standards More Secure than Passwords

OCTATCO

• Executive Summary

Here are five things we learned from this research:

① 여전히 패스워드가 가장 널리 사용되고 있는 인증 수단

② 생체 인식이 보안과 사용 측면에서 모두 주목, 긍정적 도입으로 이동하는 중

③ 사용자들은 여전히 패스워드를 강화하는 것이 계정을 보호하는 가장 좋은 방법이라고 잘못 인식

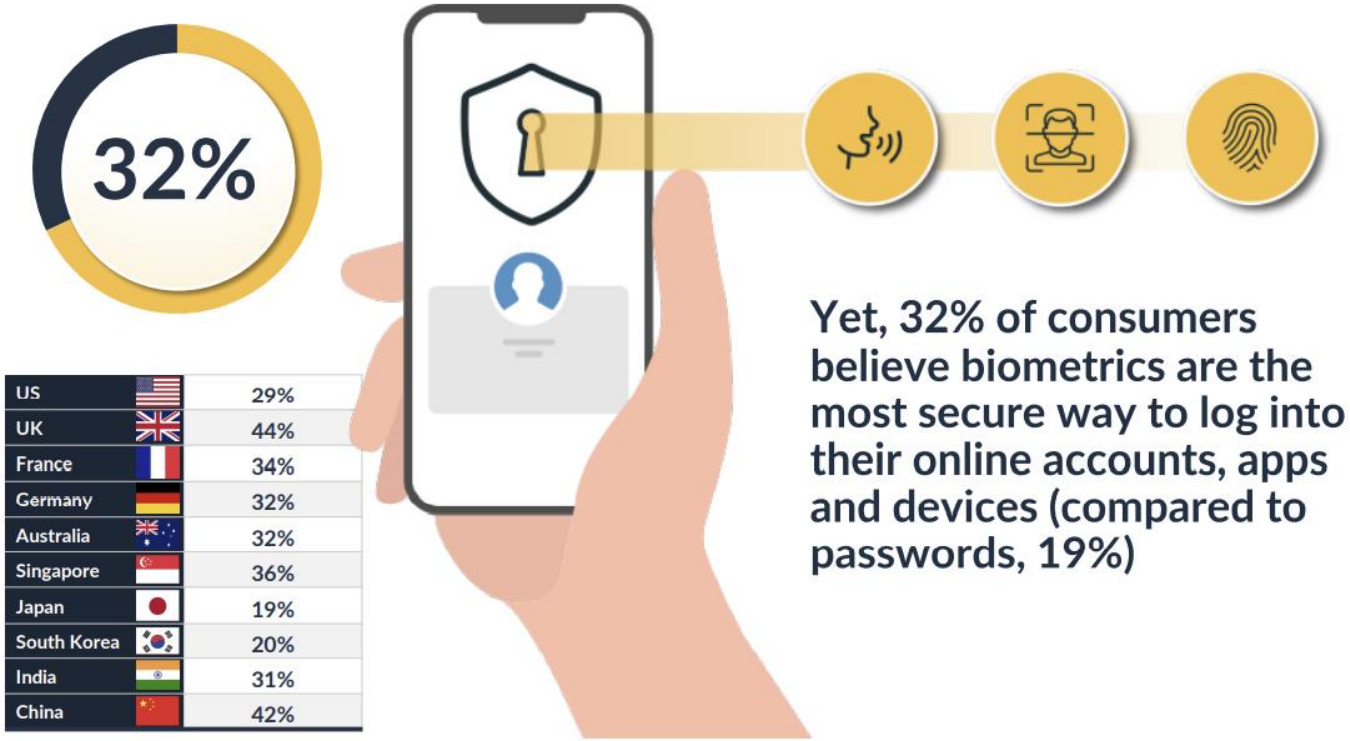
④ 다수의 고객은 도입하고 싶어도 실제로 계정을 보호하기 위한 구체적 방법에 대한 정보부족

⑤ 계정보안을 위한 솔루션 선택 방법과 부실한 계정의 위험과 영향에 대해 지속적 교육 필요

Passwords are, unsurprisingly, still the most common method of logging in across different accounts and devices.

Here's how many consumers have used a password in the past 60 days to access different accounts.

	56% Financial Services	59% Work Computer or Account	45% Social Media	38% Muli-Media Accounts such as Netflix or Spotify	27% Smart Home Devices
US	55%	55%	45%	36%	24%
UK	61%	58%	43%	38%	24%
France	58%	54%	47%	39%	22%
Germany	54%	54%	40%	31%	19%
Australia	66%	59%	42%	34%	24%
Singapore	65%	62%	52%	41%	27%
Japan	38%	52%	32%	23%	23%
South Korea	35%	51%	34%	28%	28%
India	59%	62%	58%	52%	40%
China	67%	68%	62%	57%	46%



US	29%
UK	44%
France	34%
Germany	32%
Australia	32%
Singapore	36%
Japan	19%
South Korea	20%
India	31%
China	42%

Yet, 32% of consumers believe biometrics are the most secure way to log into their online accounts, apps and devices (compared to passwords, 19%)

This could be a factor in why biometrics are the second most commonly used method for login.

Here's how many consumers have used biometrics in the past 60 days to access different accounts.

	35% Financial Services	26% Work Computer or Account	22% Social Media	16% Muli-Media Accounts such as Netflix or Spotify	19% Smart Home Devices
US	29%	20%	16%	13%	15%
UK	39%	17%	22%	13%	13%
France	26%	16%	13%	8%	7%
Germany	25%	15%	12%	7%	9%
Australia	25%	12%	15%	9%	9%
Singapore	52%	28%	24%	17%	23%
Japan	20%	26%	18%	11%	13%
South Korea	26%	26%	20%	13%	16%
India	51%	41%	35%	30%	34%
China	59%	47%	44%	35%	47%

What's FIDO Authentication?

PC

Smart Phone

Security Key

Fingerprint

Face

Iris

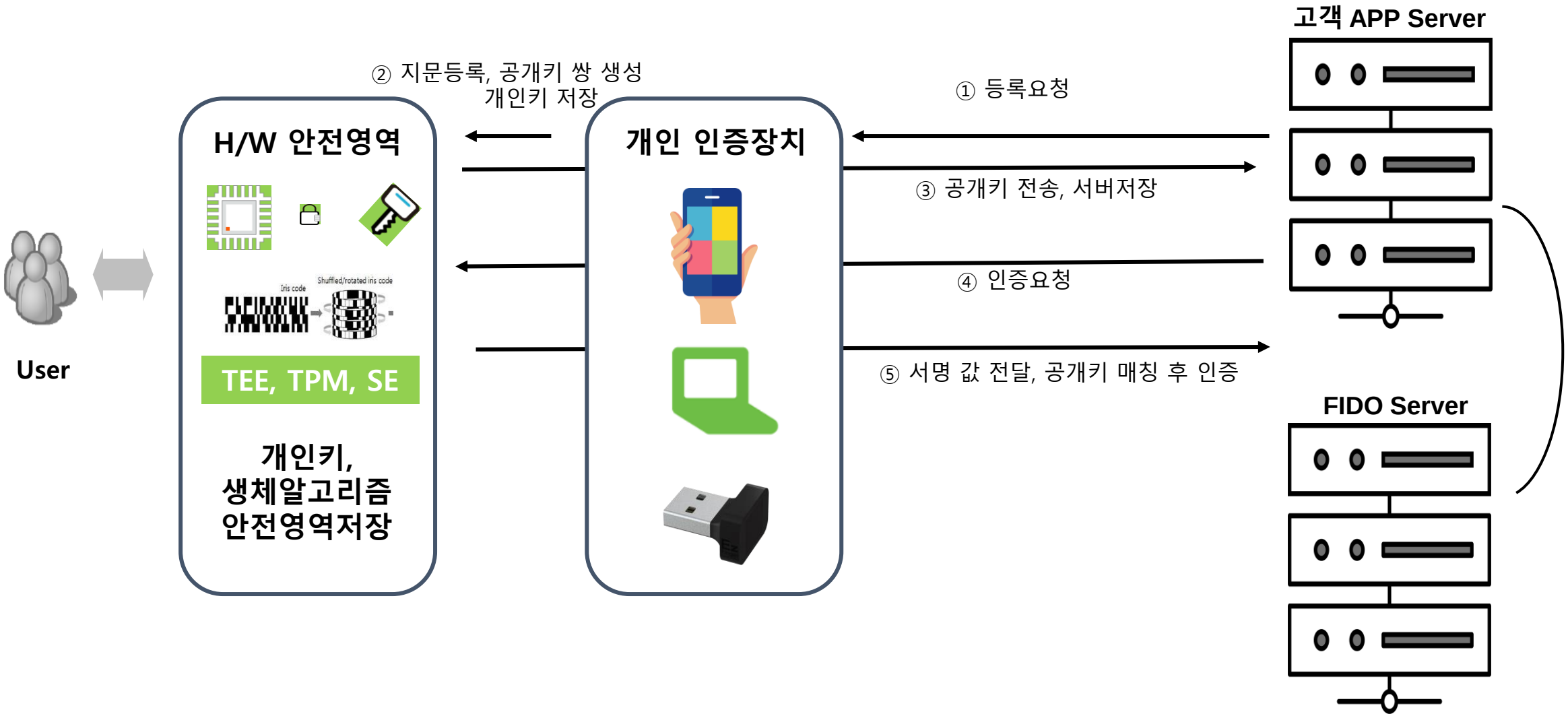
① 공개키 암호화 사용

② 인증은 H/W
개인 인증 장치로

③ 사용자 검증은 생체인식

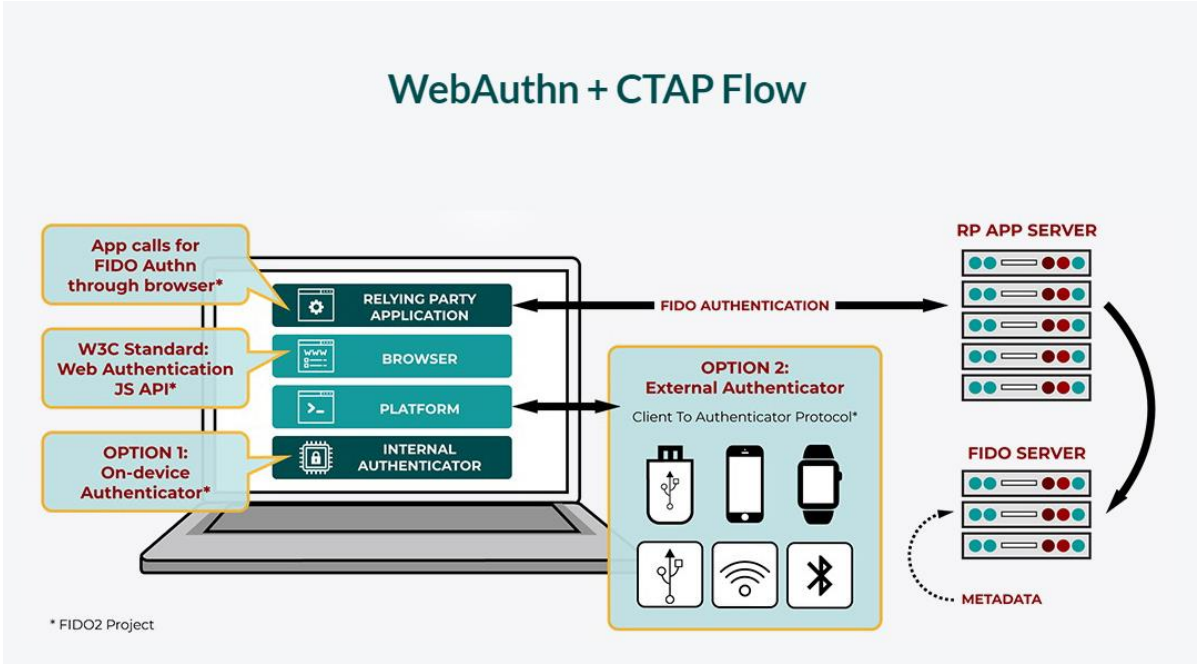
개인정보는 오직 개인의 장치에만 저장

How Strong Authentication works?



W3C(World Wide Web)+FIDO

W3C(WebAuthn)+FIDO(CTAP2)



Source: fido alliance

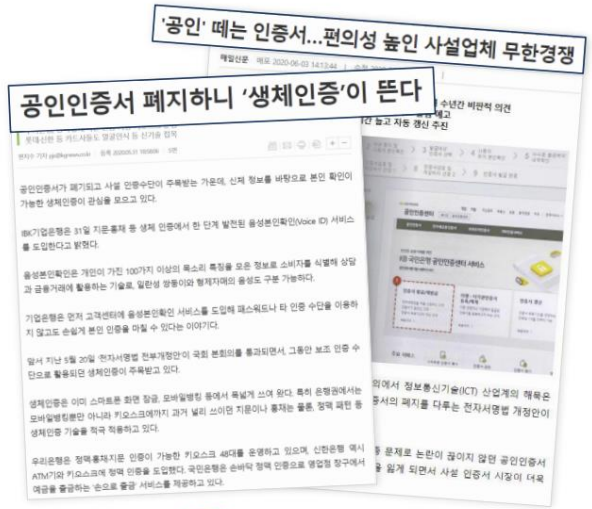
적용검토

- 패스워드 재등록 불편 감소
  - 비밀번호 재설정/복구 시도 감소
- 비밀번호 유출/스푸핑/피싱의 위험 방지
  - 비밀번호 분실 위험 감소
- 복잡한 비밀번호 정책 불필요
  - 다수의 비밀번호를 기억해야 하는 번거로움 감소

사회 환경 · 규제의 변화

비대면

본인인증의 중요성 대두!



공인 인증서

무한 경쟁, '생체인증' 기술 각광

적용범위 & 수단

1. 사업목적 수립

   예) 스마트오피스 MFA(다중인증) 도입
   사용자의 편의와 보안성을 높이고 관련 규제 충족

2. 사업범위
   예) PC로그인(로컬, AD, VDI 등)
   애플리케이션(VPN, 그룹웨어, SSO, 대고객서비스 등

3. 인증수단
   예) Passwordless or 2차 인증
   1:1 인증방식 or 1:N 인증방식
   FIDO standard 인증 or 특수목적 인증
   웹 방식 인증 or 앱 방식 인증
   스마트폰 지문, 얼굴, PIN, MOTP, 앱 인증, PC지문, 지문 보안키

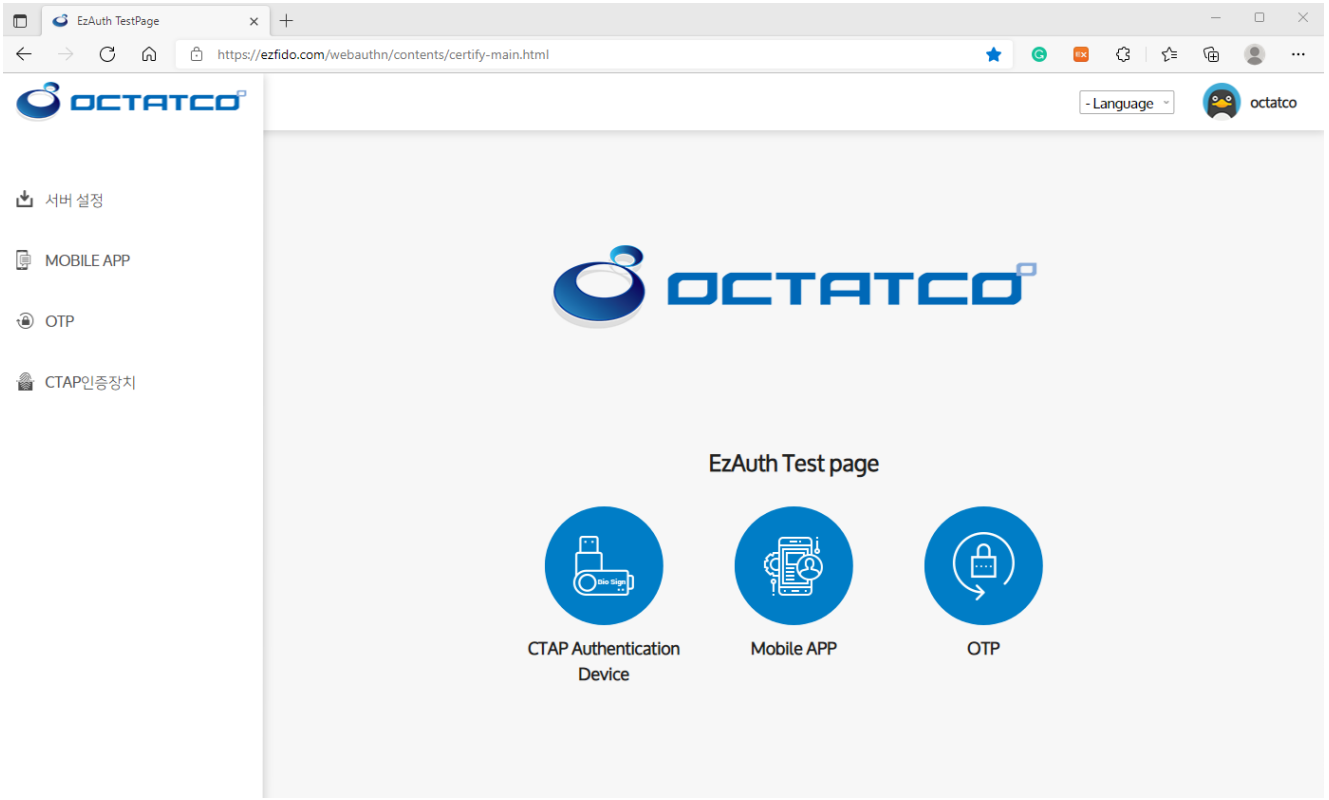
1:1 FIDO 인증 기반 상세규격 예시

○ 상세규격
- 스마트폰에 기본 탑재된 다양한 생체인증장치(지문, 안면 등) 기반의 FIDO 인증을 지원해야 함.
- 생체인증을 지원하지 않는 사용자를 위해 PIN기반의 FIDO 인증을 지원해야 함.
- USB, NFC, Bluetooth 타입의 FIDO 외부인증장치(CTAP)을 지원해야 함.
- 다양한 인증장치(스마트폰 생체인식, PIN, 모바일 OTP, 외부인증장치) 대해 **통합관리 기능**을 제공해야 함.
- APP to APP 및 In-APP 형태의 모바일 환경을 지원해야 함.
- 마켓 등록 정식앱 / SDK / 독립앱 등 고객사 선택 가능한 다양한 방식으로 Android/iOS 클라이언트 제공
- PC 환경 연동을 위해 Push, QR방식을 통한 모바일 단말기와 연동을 지원해야 함.
- Window Hello 연동을 통해, PC로그인 환경에 적용이 가능해야 함.
- FIDO 표준을 지원하는 브라우저에서는 별도 모듈 설치 없이, FIDO2의 WebAuthn 인증을 지원해야 함. (Edge, Chrome, FireFox, Safari 등)
- 서비스 연동을 위해 RESTApi 방식의 손쉬운 연동 규격을 지원해야 함.
- 웹기반 관리 기능을 통해, 사용자 및 인증장치, 인증정책에 대한 일원화된 정책관리 기능을 지원해야 함.
- 사용 현황(등록 사용자, 등록 인증장치, 인증 내역) 기능을 제공해야 함.
- 정책 관리(인증장치 허용/차단, 인증 서비스 메뉴/메뉴별 허용 인증장치, 서비스별 그룹매핑을 통한 인증정책) 기능을 제공해야 함.
- 인사정보(계열사/조직) 연동을 위해 LDAP, RDB, Excel, AD를 통한 **자동 동기화를 지원**해야 함.
- 사용자 본인이 직접 서비스별 인증장치(FIDO, OTP) **등록 및 관리가 가능하도록 셀프서비스**를 제공해야 함.
- 단말기 미소지 상황을 대응하기 위해, 관리자의 승인을 기반으로 하는 미소지자 워크플로우 기능을 지원해야 함.
- VPN 접속을 위한 2차 인증을 지원해야 하며, VPN 수정을 최소화하기 위해 RADIUS 프로토콜을 지원해야 함.
- SSO 지원여부 (ad 연동), VDI 환경 지원 가능 (CTRIX)

○ 시스템규격
- 모바일 단말 지원환경 : Android 4.4이상, iOS 9.0 이상
- 서버 지원 환경 : Unix, Linux, Windows server 등 Java 실행환경을 지원하는 OS
- Java 지원 환경 : JDK 1.8 이상 또는 OpenJDK 11 이상 지원
- DBMS 지원 환경 : Oracle 11g 이상, MySQL 5.7 이상, MariaDB 10 이상

○ 개인용 생체인증 장치 규격
- 지문인식 카드형 FIDO2 및 NFC 기능 지원 및 인증 획득한 제품
- Windows Hello 및 FIDO2 인증 획득 제품
- 전용 H/W 보안칩 Trustzone 내장 제품
- 지문인식 FRR(본인거부율) 1% 이하, FAR(타인인식률) 0.01% 충족제품
- 윈도우 10, 8, 8.1, 7 지원가능 제품
- WebauthN 지원제품

EzAuth FIDO 인증 테스트 페이지



[인증 방법]
1)EzAuth 테스트 페이지 접속
2)EzAuth App다운로드 (플레이스토어, 앱스토어)
3)EzAuth App 실행
4)PC에서 ezfido.com/webauthn 서버설정 메뉴의 QR을 EzAuth app으로 스캔
(EzAuth FIDO 통합인증서버 연동)
5)스마트폰 지문인식, PIN, OTP 인증 테스트, PC USB FIDO 지문 보안키 인증 테스트

[자사 인증시스템과 연동 테스트 webauthn API 적용, 스마트폰 지문, PIN, OTP 테스트]
1) 고객사의 로그인 페이지에서 webauthn API 사용
스마트폰 지문, PIN, OTP 인증 테스트
2) EzAuth.com에서 고객사의 URL(도메인) 도메인 설정
3) EzAuth.com/webauthn에서 모바일, OTP 등록 후 고객사의 로그인 페이지에서
로그인 실행 및 테스트
4) 고객사의 로그인 페이지에서 webauthn API인증 이후 로그인 처리.

https://ezfido.com/webauthn/contents/certify-main.html

1:N 지문인증 기반 상세규격 예시

EZF2+ _SDK v1.0.0
(Model: Ez-Finger2+ _WH)

지문인증 SDK 제공 (윈도우/리눅스 라이선스)

윈도우 Demo 동작 예시

1. 사전준비
   - EZF2+ 지문인식 보안키와 Windows Hello Driver 설치 합니다.
     [SW] EzFinger2+(이지핑거2플러스) 드라이버가 자동으로 설치되지 않을 때 – 생체인식의 모든것 octatco (웹사이트 다운로드)
   - EZF2+ 지문인식기 장치를 PC USB에 연결해주세요

2. x64>Debug>FingerPrint.exe 실행
   (이때, 관리자권한 실행)

3. Enrollment Touch 진행 후 Verify Touch 진행
   (현재 Enroll Touch 횟수는 3회 고정, 변경 가능)

4. Verify 결과 확인

보다 편리하고 안전한 인증을 위해

참고자료: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Online-Authentication-Barometer-Oct-2021, FIDO Alliance
Security - Enabling businesses for the Digital Transformation-Microsoft
NIST.SP.800-63b Digital Identity Guidance
EzAuth white paper, OCTATCO

테스트 연동문의: dwkang@octatco.com, 제품문의: sales@octatco.com , 옥타코 홈페이지: Https://www.octatco.com