

[단독] 대법원·국방부·국토부 홈페이지 맘만 먹으면 해킹..."직접 뚫어 봤습니다!" / YTN (2020.10.07)



https://youtu.be/oHRFGv_ljyo

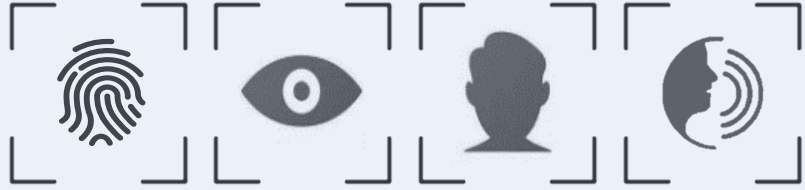
해킹 침해의 81%는 취약하거나 도난 혹은 재사용된 비밀번호로 인해 발생

MFA 보안수준은 SMS인증코드 ≤ 앱에서 생성하는 코드 ≪ 물리적 보안키

Passwordless Security Solution



FIDO (Fast Identity Online) is



생체인증(Biometrics)은 보편성, 유일성, 지속성, 측정성, 성능성, 수용성, 위·변조 불가능성 등의 조건을 충족하는 인간의 생물학적·행동적 특징을 통해 사람을 인식하고 신원을 파악하는 기술



FIDO는 공개키 기반 구조(Public Key Infrastructure)의 우수한 보안성과 생체인증의 편리성을 기반으로 비밀번호의 취약점을 개선하여 보완(MFA)하거나 대체(Passwordless)하려는 인증 프로토콜 표준



PKI기술은 공개키 암호화 및 전자서명을 기초로 클라이언트의 인증장치 (Private Key, 암호화)를 통해 생성된 인증 결과 값만을 서버(Public Key, 복호화)에서 검증하는 가장 뛰어난 암호기술

TrustKey is



표준적 범용적 지원

fido
ALLIANCE



강력한 보안성

생체정보는 자체 개발한 보안 MCU내에 암호화되어 저장

개발부터 제작까지

MCU개발, 모듈설계, 생산 & Solution



지문인증

정확성, 경제성, 이동성이 높은 생체인증

솔루션 응용

중요한 파일과 폴더를 숨기거나 암호화하여 관리



TFFM

PRECISE
BIOMETRICS

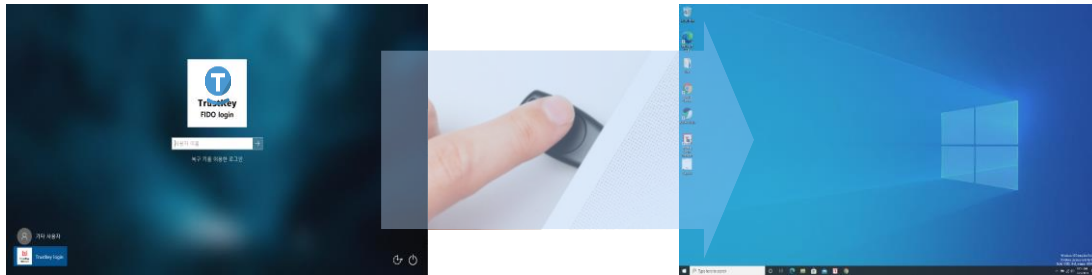
지문인식 알고리즘

신뢰받는 스웨덴의 프리사이즈 바이오메트릭스 채택

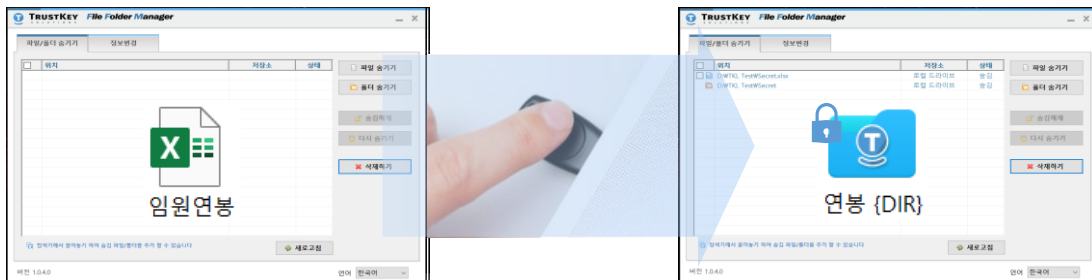
TrustKey 주요서비스



MFA (Multi-Factor Authentication) Key
FIDO를 지원하는 Microsoft Azure, Google Workspace, AWS, Citrix, Bank, SSO 등의 서비스에서 요구하는 MFA 인증을 지원하는 물리적 인증키



TKL (TrustKey Login) 솔루션
AD 도메인 로그인이나 윈도우 PC 로그인시 패스워드를 노출하는 위험없이 지문인증만으로 편리하고 안전하게 로그인 할 수 있는 내·외부망 환경 구현



TFFM (TrustKey File Folder Manager)
중요한 디지털문서를 인증키를 통해 본인임을 확인한 후 숨기거나 암호화하여 관리하며 암호화된 문서로 보고하고, 허락된 인원만이 접근할 수 있도록 응용한 암호화 솔루션

인증 방식 비교

구분	ID/Password	TrustKey	OTP Device	Mobile	인증서
기반기술	Server와 Client 값 검증	PKI & Biometrics (FIDO 2.0 Level 2)	시간동기 난수 알고리즘 비밀번호	FIDO UAF Vendor별로 상이한 기술	PKI
저장요소	Legacy Storage	전용 MCU 내 SE (Secure Element)	Legacy Storage	AP chip 내 SE	Legacy Storage
인증시간	5초 내외	2초 내외	7초 내외	10초 내외	5초 내외
보안정도	해킹 사고의 81% 차지 타인과 공유 가능	현실적 해킹 위험 없음 타인과 공유 불가능	노출 및 계산식 탈취 타인과 공유 가능	중간자 공격(MITM) 및 피싱 공격에 취약	타인과 공유 가능
분실관리	해킹에 가장 취약 복잡한 관리 지침	타인사용불가 및 복수사용 분실시 간편한 백업 절차	분실시 신고 및 재등록 타인 사용 가능	공사 구분이 모호 분실시 복잡한 복구 절차	신고 및 재발급
유지비용	표면적 비용은 없으나 내재적 비용 측정 불가	초기 도입 비용	배터리 수명에 의한 교체수요	초기 도입 비용 Vendor Lock-in 비용	유효성 검증을 위한 비용 (Option)
특장점	전통적 비휴대성	보안성 및 이동성 발전가능성	보안성	휴대성 및 포괄성	특정시장 지배성

생체인증 기반의 FIDO 인증 방식이 보안성, 편의성 및 경제성에서 모두 우수한 솔루션 구현

TrustKey 도입 효과 및 적용 분야

비밀번호 노출 없이 보안성 강화

- ✓ 지문방식으로는 세계 최초이며 유일하게 FIDO2.0 Level 2 보안등급 획득
- ✓ FIDO 지문인증 기반으로 비밀번호 노출이 없고, 제품내 보안 MCU에 지문 정보를 저장하여 외부 유출이 불가

편리하고 간편한 로그인

- ✓ Passwordless를 구현하여 입력 없이 터치 한번으로 On·Off Line 및 내·외부망에 하나의 인증키로 로그인 가능

관리의 편리성

- ✓ FIDO 표준을 준수하므로 Vendor Lock-in에서 자유롭고 종속되지 않음
- ✓ 한번의 지문 등록으로 계정 생성과 로그인이 가능하며 인사이동에 빠르게 대응
- ✓ 정기적인 비밀번호 재설정(사용자) 및 관리 정책(관리자)의 피로도를 획기적으로 개선

적용분야

- ✓ Mobile 기반 FIDO 서비스의 한계 보완
- ✓ Login 보안 강화를 필요로 하는 솔루션, 기업, 공공기관, 정부기관
- ✓ 운영체제, 클라우드, 인터넷서비스 및 금융 거래, 보안 제품의 2단계 인증 또는 대체 인증 솔루션 수요

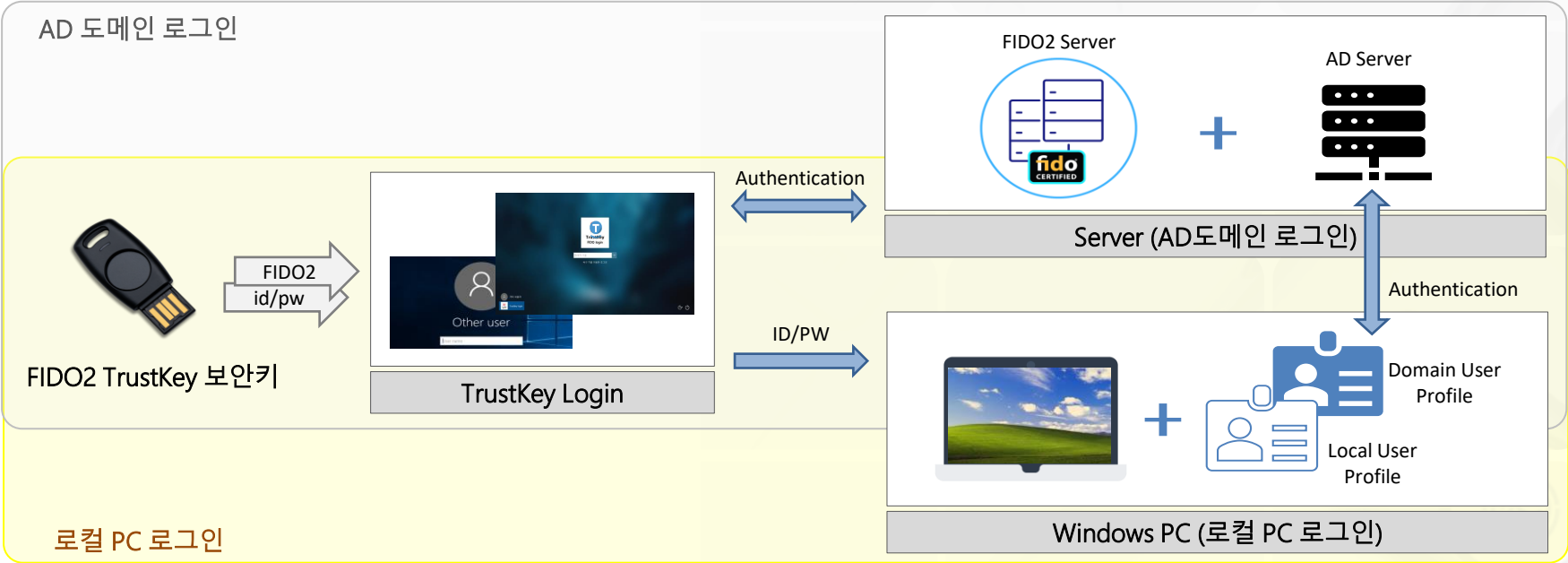
주요 공급 및 진행 사례

고객	시기	목적	제품
 대한민국 청와대	2020년	내부망 로그인 보안 강화 및 Passwordless 인증	FIDO Svr / G310 Key TrustKey Login solution
 한국수력원자력주	2020년	업무 Portal 로그인 및 FIDO 2차 인증 사용자 인증 강화	G500 / G310 UAF Key (FIDO2 authenticator)
 외교부 Ministry of Foreign Affairs	2021년	외교부정보전용망 구축 프로젝트 도입(2022.1~) (서울, 북미, 일본 등 직원 로그인 보안 및 사용자 인증 강화)	FIDO Svr / G310 Key TKL solution
 BANK OF AMERICA	2021년 ~	B2C 대상으로 \$500 이상 송금시 FIDO 2차 인증 적용 은행 고객 대상 FIDO 보안키 판매	T110 / G310 / G310H Key (U2F/FIDO2 authenticator)
 AUSTIN Independent School District	2021년	미국 텍사스 오스틴 지역 학군 (초, 중, 고 129개 학교) Passwordless 로그인 인증으로 FIDO 보안키 적용	T110 Key
 amazon web services™	2022년	Root 계정 FIDO 2차인증 사용자 복수 사용	T110 Key
 TAPPIN	2021년 ~	가상자산 및 플랫폼 보안 인증 / Passwordless 인증 TFFM 솔루션 적용	G310H / G320H Key TFFM / TKL solution

대표사례. TrustKey Login 솔루션 적용 (BH)

목적	생체 인증 보안 솔루션을 이용하여 해외 출장 및 사내 근무시 PC 보안 시스템 (Passwordless) 구축	
대상	해외 출장용 노트북 및 내부직원 각 PC 2대 (내부망/외부망)	
계정정보	AD Server (AD 연계로 개방적이고 확장성 큼)	
적용	<u>요구사항</u>	<u>구현내용</u>
	• 패스워드를 사용하지 않는 신뢰할 수 있는 제품일 것 • 표준을 따르고 원천 기술일 것 • 구현 솔루션 중 가장 높은 보안 등급을 적용할 것 • 보안성 강화 및 외부 도용을 방지할 것 • 내·외부망을 모두 지원할 것 • PC, Server 또는 Storage에 정보를 저장하지 말 것 • 기존 계정관리 솔루션과 연동 및 통합 인증정보 구성	• Passwordless / Made in Korea • FIDO2 / MCU개발, 모듈설계, 생산 & Solution • 세계 최초, 현재 유일의 FIDO 2.0 Level 2 보안 등급 • 지문 생체인증 방식의 보안 인증키 / 1인 1키 • 하나의 인증키로 내·외부망을 모두 지원 • 인증키의 MCU내에 지문정보 암호화 관리 • AD Server 연계 / AD외 계정관리솔루션에 API 제공
주요기능	• 모든 사용자는 PC에서 업무가 가능하며 순방 및 출장업무 등에 최적화된 기능 제공 • 사용자 및 인증키의 정보 조회, 등록, 수정, 삭제, 인증 이력 및 오류 조회 기능을 제공하여 인증정보 통합 관리시스템을 구현 • 장애 발생시 대응 관련 백업 및 복구방안 기능 제공 • On-line, Off-line 환경에서 모두 로그인 가능	
결론	고객의 만족도가 높고 솔루션 확대 적용 가능성	

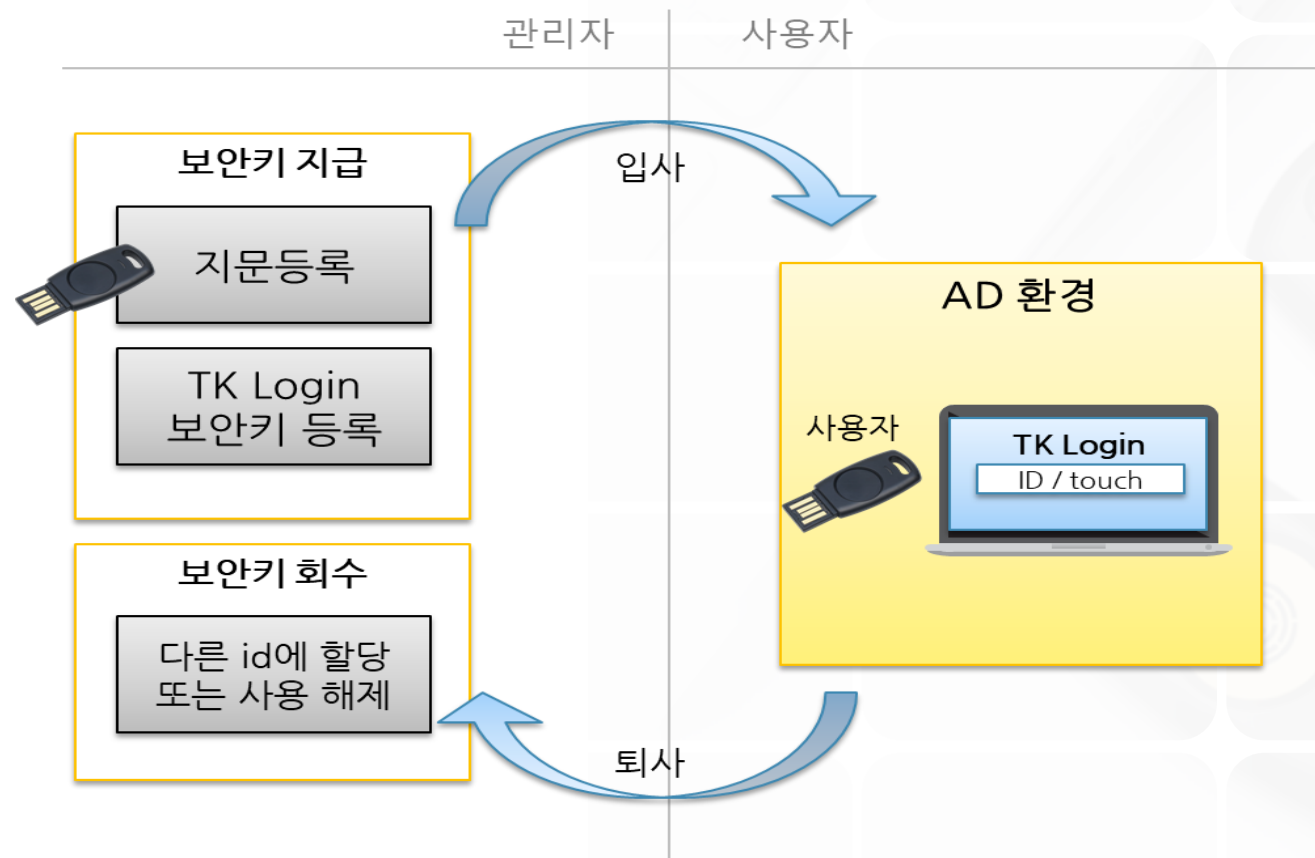
대표사례. TKL 동작 Diagram 및 구성 기능 (BH)



TKL Application	- FIDO Security Key 로그인 기능 : AD(Domain) 계정 로그인, Windows Local 계정 로그인 - Windows Logon Application Plug-in으로 지문인식 인증키 로그인 지원 - 긴급 복구 로그인 지원 : 관리자용 Recovery Code 생성 및 로그인 지원
TKL Manager	- AD 사용자 검색 및 식별, 사용자 ID에 인증키 등록 - AD 계정 연결 : Server IP, Group/Domain name 입력, 로그인 정보 입력시 계정 목록 가져오기 - Windows 사용자 ID-인증키 등록 : 등록 시나리오에 따라 사용자 ID와 보안키 연결 등록
TKL RP Server	- Dashboard : 사용자 정보 표시 및 조회 (ID, 인증키 S/N, 로그인 이력 등) - 시스템 : 인증키 및 사용자 관리, 관리자 기능에 따른 인증키 설정 및 비밀번호 설정 등
TKL Server	FIDO2 Server 연동 및 표준에 따라 인증키에 대한 정보를 유지 및 관리

대표사례. TKL 사용 시나리오 (BH)

입사시 인증키 지문 등록 및 계정 생성(파일 설치) ⇨ 내·외부망 및 출장시 TKL사용 ⇨ 분실 및 미소지시 Recovery Code 제공
⇨ 인증키 정보 조회, 등록, 수정, 삭제, 오류 및 이력 등 인증정보 통합 관리 ⇨ 퇴사시 키 회수 / 미 회수시 사용 해제 / 공장초기화



참고. FIDO에 관한 주요 보도자료 (국가정보원)

국가정보원(NIS) 국가보안요구사항 V3.0 배포 (2021.09)

국가용 보안요구사항은 제품이 구현해야 하는 모든 보안 기능이 아닌 기본적으로 만족해야 할 사항을 기술한 문서입니다. 개발업체는 최신 보안위협에 대응하기 위해 국가용 보안요구사항의 항목 뿐 아니라 추가적인 보안기능 구현을 통해 제품의 보안성을 제고할 것을 적극 권고합니다.

1.1.2

조건부 필수	제품은 사용자 식별 및 인증을 위해 1.1.1과 병행하여 추가적인 식별 및 인증 기능을 자체 또는 외부 IT실체와 연동하여 제공해야 한다.
조 건	추가적인 식별 및 인증 방식 지원시

요구항목

- ① 추가적인 식별 및 인증 기능 제공을 위해 △FIDO 표준을 준수한 2FA 지원 기기 △인증서 △일회용 비밀번호 생성기(OTP) 등을 활용할 수 있다.
 - 제품 · 운용환경에서 지원할 경우 'FIDO 표준을 준수한 2FA 지원 기기'를 권고한다.

국정원, 공공분야 보안제품에 '생체인증' 기본 탑재 추진 (ZDNet Korea, 2022.06.11)

IT보안업계 대상 '보안적합성 검증정책 설명회'서 계획 공개
국가정보원이 국가·공공 기관이 도입하는 IT 보안제품에 대한 사용자 인증체계 전면 개편을 추진한다.

현재는 아이디와 패스워드 인증을 기본으로 하고, 추가적으로 생체인증을 할 수 있도록 되어 있다. 이를 FIDO나 생체인증을 기본으로 하고 핀 번호나 아이디·패스워드를 부가적으로 사용하게끔 변경한다는 계획이다.

국정원 관계자는 “국가지원을 받는 해킹 조직들이 아이디와 비밀번호를 탈취하는 것을 주요 목표로 활동 중”이라며 “이에 국가기관 IT 운용 관리의 안전성을 강화하기 위해 사용자 인증체계 개편을 추진한다”고 설명했다.

국정원은 보안 업체들이 제품 개발에 시간이 소요될 수 있다고 보고, 유예기간을 적용해 개편을 추진한다는 계획이다.

FAQ. 기존 보안제품과 비교 질문

기존 보안 제품	기존 보안의 특징	기존 보안의 단점	지문 보안키의 장점
OTP SMS Mobile	난수발생, 범용적 문자 메시지로 2차 인증 사용 Mobile 앱, 편리성	불편함, 타인 사용 가능 입력시 피싱 및 중간자 공격 취약 기능 집중화 및 사용 제한 구역 존재	타인 사용 불가 부인 방지 기능 불법 로그인 불가로 정보탈취 불가 개인별 보안키 지급으로 보안성 강화
폐쇄망	외부망 접근 불가	비밀번호 인증 및 내부자 동조	
네트워크 접근제어 (NAC)	네트워크 접근을 막아 외부 침입 봉쇄	비밀번호 공유 및 타인 사용 가능	
가상사설망 (VPN)	접속을 위한 네트워크 터널링 보안		
통합인증 (SSO)	보안의 향상없이 편리성 증대	2차 인증 불편함 및 비밀번호 공유	

질문 내용	담당자 의견	지문 보안키 답변
지문 인증 사용 경험과 시스템이 있다.	인식율이 낮아 불편하다.	빛에 취약한 광학식이 아닌 정전식으로 인식율 99.9%
노트북의 Built-in된 지문 장치와 다른가?	동일한 것이 아닌가?	Built-in 제품은 지문정보를 노트북에 저장
Windows Hello 지문과 차이점은 무엇인가?	Windows Hello 지문으로 로그인 하고 있다.	스캐너 이용 방식이며 이동성이 없음
지문 인증 시스템이 있다.	지문정보를 서버나 PC에 저장하는 시스템을 사용한다. 지문 정보 보관방식이 불안하다.	기존 시스템은 구조가 복잡하여 유지보수가 어려움 FIDO는 도입 및 유지보수가 용이하고 보안성이 우수

FAQ. 자주 받는 질문 내용

질문 내용	기존 보안 제품	지문 보안키
FIDO가 무엇인가?	비밀번호 및 보안기기의 문제점을 해소하기 위하여 Passwordless를 모토로 출범하여 ITU(국제전기통신연합)의 승인을 받은 국제 보안 인증 프로토콜	
제조 국가가 어디인가?		100% Made in Korea
잃어버리면 어떻게 하나?		타인 사용이 불가하며 새로운 키로 등록 및 대체 가능
지문정보는 어디에 보관하나?	서버 및 클라이언트에 저장되어 보안성이 낮음	보안키 내부의 보안칩에 암호화 하여 안전하게 저장
도입이 어렵지 않나?	서버 도입시 장기간 프로젝트로 결정이 난해	표준제품이므로 도입이 쉽고 도입기간이 매우 짧음
기존 Legacy 시스템과 연계의 어려움은?	매우 복잡	키, Protocol, Server가 표준으로 상용제품에 기 구현
AD를 사용하는 경우 도입 방법은?	AD 연동이 복잡하고 쉽지 않음	Windows의 기본 AD 로그인을 그대로 사용 호환성과 연계성이 뛰어남
계정관리 서버가 없는 경우에 구성이 가능한가?	대부분 표준을 따르지 않아 Vendor Lock-in 효과	API제공 / On-Premise 키관리 서버 도입 PC별로 로그인 프로그램을 설치하여 구성 (TKL)
사용 가능한 OS 제한이 있는가?		대부분의 최신 OS에서 직간접 지원 Windows, MacOS, Linux, Android, iOS, Chrome
PC에서만 사용이 가능한가?		젠더 사용으로 대부분 사용 가능
어디에 활용이 가능한가?		OS, 웹사이트, 앱, Cloud, 은행, SSO, Passwordless

트러스트키는 FIDO 기반의 지문 생체인증 방식을 USB 인터페이스로 구현한 보안 인증키입니다

TKL은 FIDO 시스템을 구축하고 인증키를 이용하여 Passwordless 업무환경을 구현하는 솔루션입니다.

QnA

영업 문의는 오수일 매니저 (Mobile 010·3297·4667 / email sioh@ewbm.com)

마케팅 문의는 전대진 매니저 (Mobile 010·7585·2530 / email david@ewbm.com)

기술·개발 문의는 홍영석 연구소장 (Mobile 010·3286·9188 / email yshong@ewbm.com)

<https://trustkey.kr>