사용자 인증을
필요로 하는
모든 서비스

Ydentity2.0

Next Authentication Platform
Whykeykey

CONTENTS

01 인증 트렌드의 변화

02 솔루션 소개

03 주요 기능

04 솔루션 특징

05 도입 사례

06 구축 및 유지보수

07 와이키키소프트 소개

01

인증 트렌드의 변화

01

컴퓨터 앞 **최대 위기 상황**

비밀번호 오류

입력한 비밀번호가 틀렸습니다.
정확한 비밀번호를 다시 입력하십시오.
연속 5회(현재 1회 남음) 오류 시 재등록 절차가 필요합니다.

확인

비밀번호 유출

방금 사용한 비밀번호가 정보 유출로 인해 노출된 것으로 확인됩니다. 계정을 보호하려면 저장된 비밀번호를 변경해 주시기 바랍니다.

비밀번호 변경

계정 해킹 시도

의심스러운 로그인이 시도되었습니다.
보안상 안전하지 않은 방법으로 로그인 시도가 감지되어 안전상의 이유로 새로운 비밀번호로 변경해 주시기 바랍니다.

비밀번호 변경

다양한 인증수단이 등장하지만… 근본적이지 못한 변화 시도들

보안수준 향상보다는 불편만 야기

Passwordless Authentication

비밀번호 문제를 해결하는 가장 좋은 방법은

비밀번호를 사용하지 않는 것

Microsoft

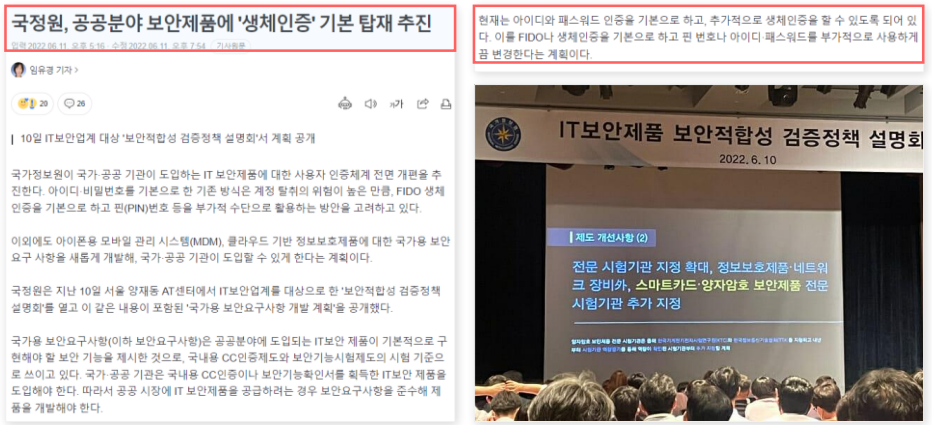
Windows Hello를 시작으로
Edge브라우저에서 FIDO인증을 지원하여
OS부터 웹서비스의 모든 영역으로 확대 중

iOS, 별도의 동글 인증장치 지원을 시작으로
macOS에서도 WebAuthn기반
FIDO2 인증장치를 지원

Google

Android 및 Chrome 브라우저에
표준 패스워드리스 인증 API 탑재

사회 환경 · 규제의 변화로 인증 보안 시장도 변화


국정원, 공공분야 보안제품에 '생체인증' 기본 탑재 추진

임유경 기자

10일 IT보안업계 대상 '보안적합성 검증정책 설명회'서 계획 공개

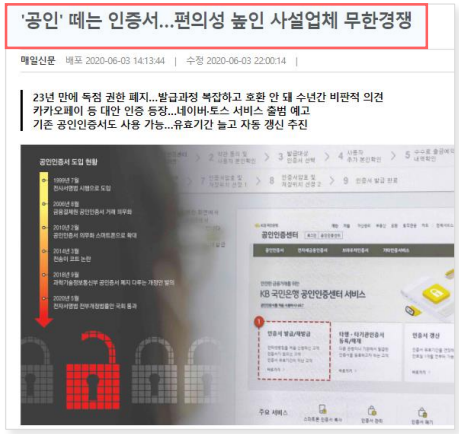
국가정보원이 국가·공공 기관이 도입하는 IT 보안제품에 대한 사용자 인증체계 전면 개편을 추진한다. 아이디·비밀번호를 기본으로 한 기존 방식은 계정 탈취의 위험이 높은 만큼, FIDO 생체인증을 기본으로 하고 핀(PIN)번호 등을 부가적 수단으로 활용하는 방안을 고려하고 있다.

이외에도 아이폰용 모바일 관리 시스템(MDM), 클라우드 기반 정보보호제품에 대한 국가용 보안요구 사항을 새롭게 개발해, 국가·공공 기관이 도입할 수 있게 한다는 계획이다.

국정원은 지난 10일 서울 양재동 AT센터에서 IT보안업계를 대상으로 한 '보안적합성 검증정책 설명회'를 열고 이 같은 내용이 포함된 '국가용 보안요구사항 개발 계획'을 공개했다.

국가용 보안요구사항(이하 보안요구사항)은 공공분야에 도입되는 IT보안 제품이 기본적으로 구현해야 할 보안 기능을 제시한 것으로, 국내용 CC인증제도와 보안기능시험제도의 시험 기준으로 쓰이고 있다. 국가·공공 기관은 국내용 CC인증이나 보안기능확인서를 획득한 IT보안 제품을 도입해야 한다. 따라서 공공 시장에 IT 보안제품을 공급하려는 경우 보안요구사항을 준수해 제품을 개발해야 한다.

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.


'공인' 떼는 인증서...편의성 높인 사설업체 무한경쟁

매일신문 배포 2020-06-03 14:13:44 | 수정 2020-06-03 22:00:14

23년 만에 독점 권한 폐지...발급과정 복잡하고 호환 안 돼 수년간 비판적 의견
카카오페이 등 대안 인증 등장...네이버·토스 서비스 출범 예고
기존 공인인증서도 사용 가능...유효기간 늘고 자동 갱신 주진


공인인증서 폐지하니 '생체인증'이 뜬다

IBK, 지문 등서 한단계 발전 '음성본인확인' 도입
우리은행, 정맥·홍채·지문 인증 가능 키오스크 운영
롯데신한 등 카드사들도 얼굴인식 등 신기술 접목

공인인증서가 폐기되고 사설 인증수단이 주목받는 가운데, 신체 정보를 바탕으로 본인 확인이 가능한 생체인증이 관심을 모으고 있다.

IBK기업은행은 31일 지문·홍채 등 생체 인증에서 한 단계 발전된 음성본인확인(Voice ID) 서비스를 도입한다고 밝혔다.

음성본인확인은 개인이 가진 100가지 이상의 목소리 특징을 모은 정보로 소비자를 식별해 상담과 금융거래에 활용하는 기술로, 일란성 쌍둥이와 형제자매의 음성도 구분 가능하다.

기업은행은 먼저 고객센터에 음성본인확인 서비스를 도입해 패스워드나 타 인증 수단을 이용하지 않고도 손쉽게 본인 인증을 마칠 수 있다는 이야기다.

앞서 지난 5월 20일 '전자서명법 전부개정안'이 국회 본회의를 통과되면서, 그동안 보조 인증 수단으로 활용되던 생체인증이 주목받고 있다.

생체인증은 이미 스마트폰 하면 잠금, 모바일뱅킹 등에서 폭넓게 쓰여 왔다. 특히 은행권에서는

보안 강화

국정원, 공공 보안제품에 '생체인증' 기본 탑재

공인 인증서

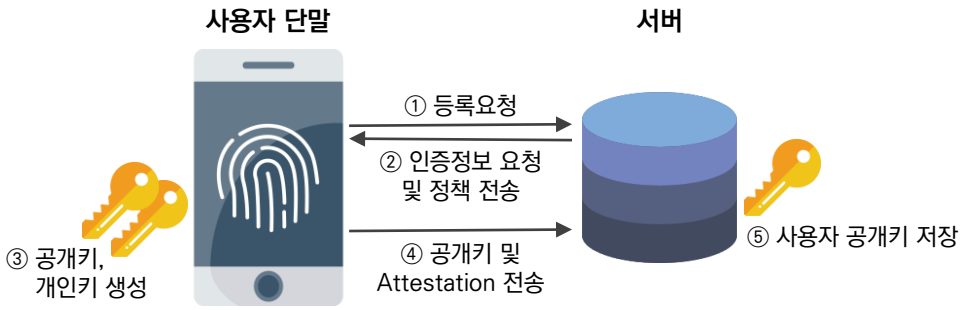
안전하고 편의성 높은, '생체인증' 기술 각광

FIDO에 대한 이해

“비밀번호 보안 취약성 등 문제점을 해결하기 위한 Passwordless 방식 인증 프레임워크”

fido™ ALLIANCE | simpler stronger authentication

- 생체인식 기술 등을 포함한 **인터넷 인증기술의 표준 정립**을 목적으로 2012년 7월 설립된 협의회
- 회원사 : 삼성전자, LG전자, 크로셜텍, 구글, 마이크로소프트, 페이팔, BC카드 등
- 2014년 12월 9일 FIDO 1.0을 공개
- 2018년 4월, FIDO 2 공개



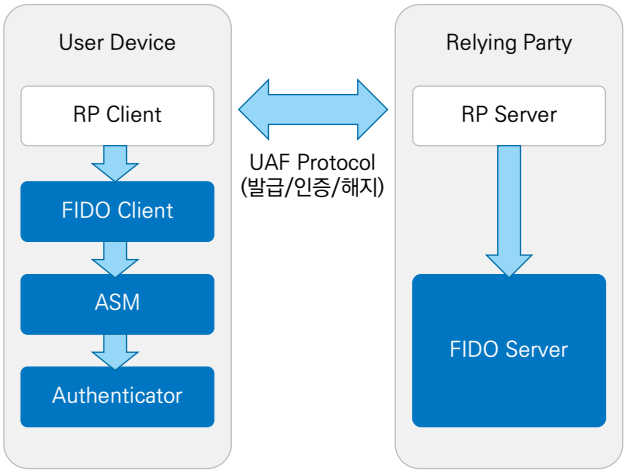
1. 단말기가 서버에 인증 요청
2. 인증을 위한 Challenge 값을 단말기에 전달
3. 단말기는 개인키를 추출하여 Challenge 값 전자서명
   - 개인키 추출: 단말기 로컬에서 생체인증 수행 후 인증 성공 시, 개인키 추출
   - 개인키? : PKI기술에서 전자서명을 수행하기 위한 키로 쌍이 되는 공개키를 서버에서 가지고 있음
4. 전자서명을 서버에 전달
5. 서버는 전자서명을 검증하고 인증 여부 결정

인증기법과 그 인증정보를 주고 받기 위한 **인증 프로토콜을 분리**하는 것이 핵심

FIDO에 대한 이해

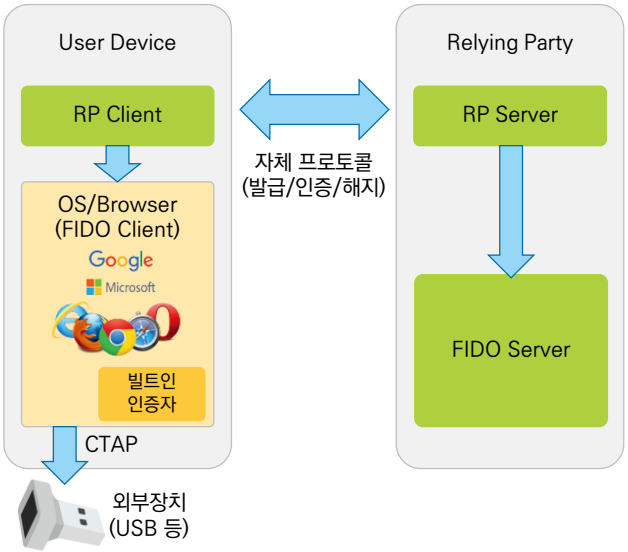
“모바일만 가능했던 FIDO1.0에서 FIDO2는 PC/Web 환경까지 인증 확대”

FIDO 1.0



- FIDO 1.0은 모바일을 중점적으로 사용(안드로이드, iOS 모바일 앱)
- 통신 방식 – UAF 프로토콜(U2F는 Chrome에서만 지원)
- Authenticator / ASM / Client와 Server로 구성

FIDO2



- FIDO2는 플랫폼(OS 및 웹 브라우저)에 FIDO가 탑재
  (Authenticator/ASM/Client가 플랫폼에 포함)
- 통신방식 – 서버에서 정의한 자체 프로토콜
- 별도의 외부 인증장치(Authenticator) 사용 가능
  (외부인증장치는 CTAP(USB, NFC, BLE 등) 프로토콜 사용)

“Passwordless를 구현하여 사용자 및 관리자 측면의 모든 스트레스를 해소”

PW 재등록 불편함 감소

01

02

유출/도용 위험 제거

PW 분실 리스크 감소

03

04

PW 기억 불필요

PKI 기반 암호화 탑재

05

06

PW 정책관리 불필요

- 자리 수 제한
- 만료기한 설정
- 특수문자 입력
- 영대문자 입력
- 입력제한(생년월일, 연결숫자 등)

PW 주기적 변경 불필요

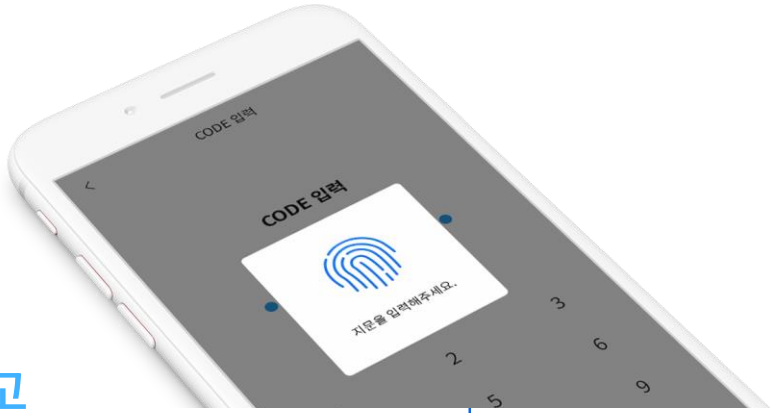
07

02

솔루션 소개

02

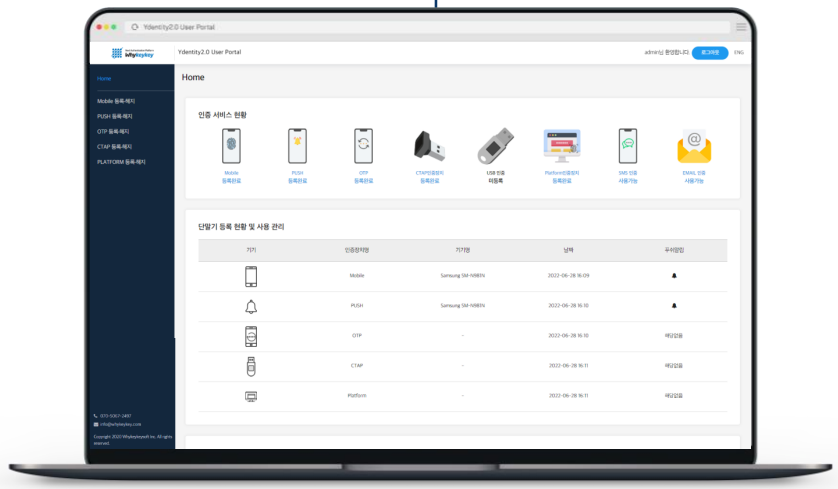
Ydentity2.0의 『초』간편 보안인증 방식



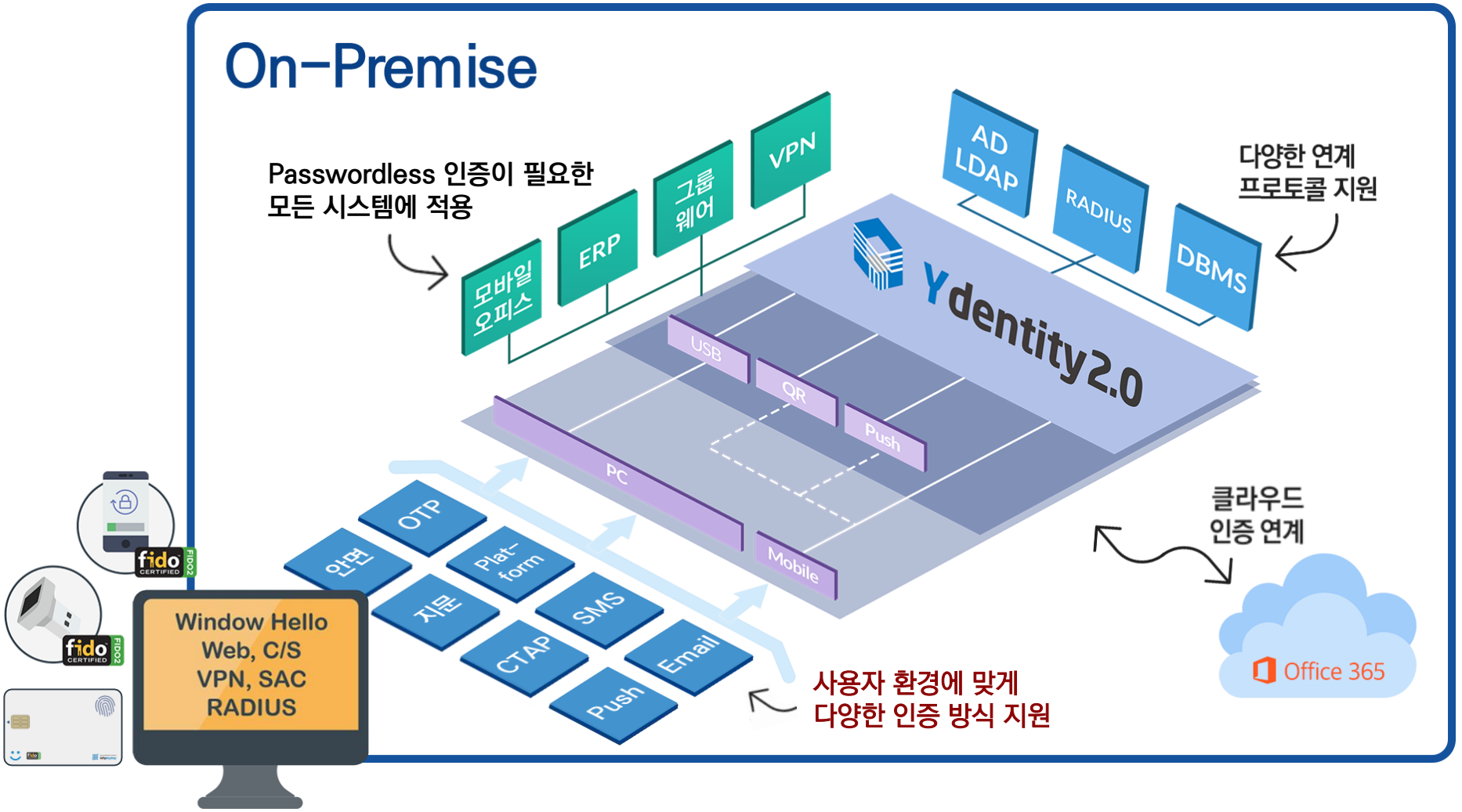
01 아이디만 입력하고

02 인증만 하면?

03 로그인 완료!

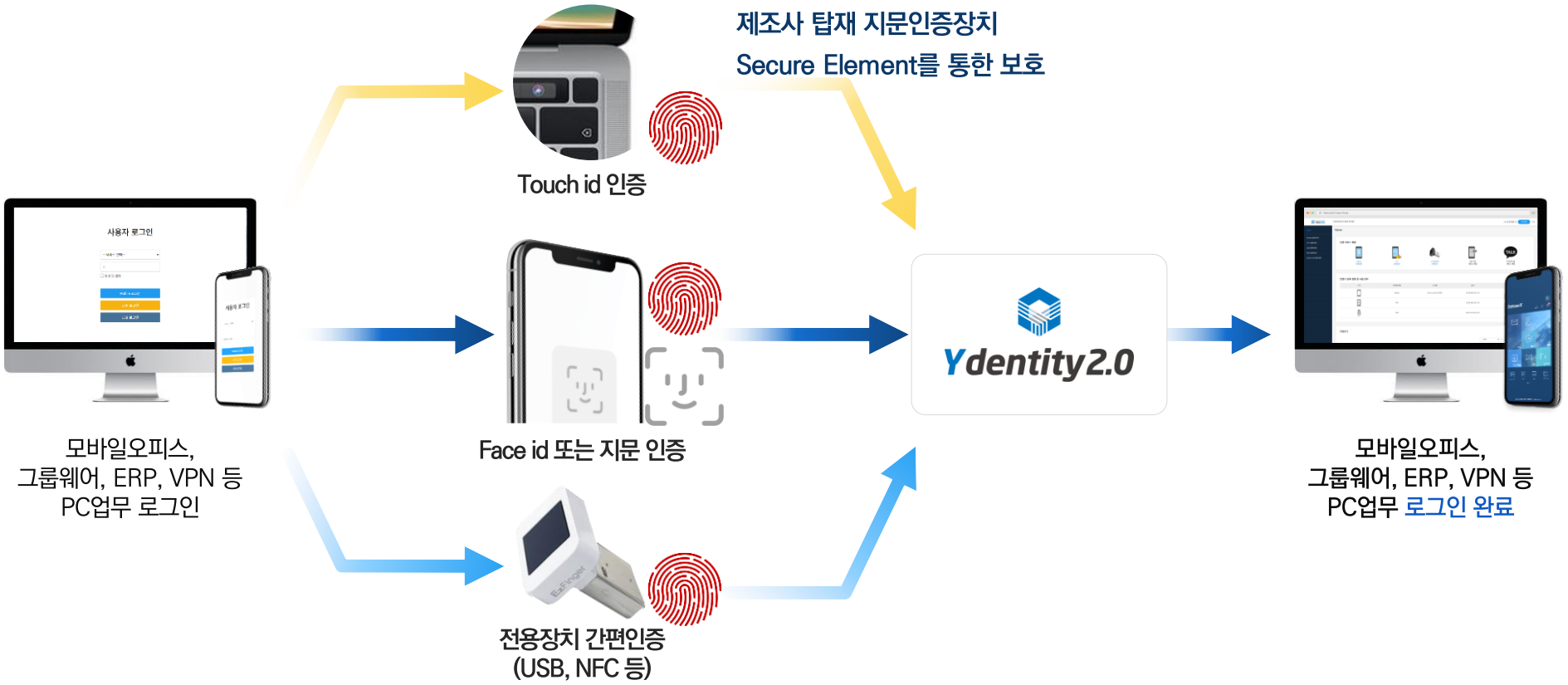


Ydentity2.0을 통한 통합인증 모델 수립



스마트폰/CTAP을 통한 간편인증 프로세스

모바일 오피스 및 ERP, 그룹웨어, VPN과 같은 회사의 업무 시스템의 인증을
FIDO2 생체 인증 방식을 통해 간편하고 안전한 Passwordless 환경으로 구현합니다.



생체인증 미지원 폰에 대한 다양한 인증 지원

생체인증 미지원폰 사용자를 대비하여 FIDO 인증 외에도 OTP, Push, SMS, Email 인증과 2차 인증 방식이 필요한 경우에도 적용 가능합니다.

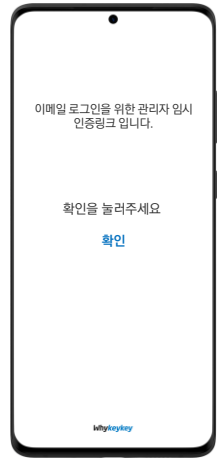
OTP 인증

Push 인증

SMS 인증

PIN 인증

Email 인증



범용성 강화

Push, OTP, SMS, Email 등
다양한 인증수단 추가제공으로 생체 인증
미지원 단말에서도 편리하고 안전한
인증 환경을 제공

Legacy 인증 환경 확대

2G폰 사용자 환경 보장 및 기존 SMS,
OTP 인증 환경의 수용을 통해
Legacy 환경의 최소 변경으로 적용 및 구축
가능

통합 관리

Ydentity2.0를 통한 다양한 인증수단에 대해
통합 정책 관리기능을 통해
관리성 향상 및 효율성을 강화

03

주요 기능

03

“Ydentity2.0 패키지 구축/SDK(API) 제공을 통한 구축”

솔루션	방법론	구성	설명
Ydentity2.0 솔루션	와이덴터티 솔루션 제품 구축 및 사용	Admin Portal	FIDO2 인증 사용을 위한 서비스설정 및 인증정책 등 관리를 위한 포탈
		User Portal	FIDO2 실사용자가 서비스의 인증정책에 따른 인증 등록을 위한 유저 포탈
		Mobile 생체인증 로그인 (FIDO2)	Android Client / iOS Client 모바일을 이용한 FIDO2 생체 인증 로그인
		Mobile Push 로그인	생체인증이 없는 스마트폰에서도 인증 가능하도록 Push를 이용한 인증 방식
		FIDO2 전용 인증장치(CTAP) 로그인	FIDO2 인증을 지원하는 웹브라우저와 OS기반에서 전용장치로 생체 인증할 수 있는 방식
		Mobile OTP 로그인	보안 강화를 위한 모바일 OTP를 이용하여 1차 및 추가 인증을 하는 방식
		Platform 인증장치 로그인	Windows Hello와 MacOS Platform에서도 로그인 가능하도록 지원
		SMS 로그인	등록된 사용자 Phone의 SMS로 인증코드를 발송하여 로그인하는 방식
		Email 로그인	등록된 사용자의 Email에서 인증 후 로그인 가능하도록 하는 방식
		FIDO2 Radius Protocol	VPN 등과 같이 별도의 커스터마이징 없이 자체 Radius만으로 FIDO 인증할 수 있는 프로토콜
		공용 인증장치 로그인	ID/PW 없이도 공용 인증장치가 있는 어디서든 생체 인증만으로 로그인할 수 있는 모듈
Ydentity2.0 SDK	lib, SDK 제공하여 고객사 제품에 내재화	FIDO2 Server SDK	고객사 자체 솔루션에 FIDO 서버를 내재화 하기 위한 SDK
		FIDO2 Android Mobile SDK	고객사 자체 Android 기반 모바일에 FIDO 내재화를 위한 SDK
		FIDO2 iOS Mobile SDK	고객사 자체 iOS 기반 모바일 FIDO 내재화를 위한 SDK
		FIDO2 Windows Client App SDK	윈도우 기반 앱에서 FIDO 인증을 가능하도록 내재화를 지원하는 SDK
		FIDO2 macOS Client App SDK	macOS 기반 앱에서 FIDO 인증을 가능하도록 내재화를 지원하는 SDK

Ydentity2.0 솔루션 – “FIDO2 구축형 제품을 고객사 솔루션과 연동!”

- Admin & User Portal
- Mobile App for Android/iOS
- Mobile Push
- 전용 인증장치 (CTAP)
- Mobile OTP
- SMS & Email
- Windows & macOS 내재장치 인증
- 서버방식 공용장치 인증

주요 기능 리스트

솔루션	구분		세부 규격
Ydnetity 2.0	Client	인증장치	단말기에 기본 탑재된 FIDO 기반의 생체인증장치(지문, 안면 등) 인증 가능
			USB타입 등 FIDO 기반의 외부인증장치(CTAP) 인증 지원
		추가인증수단	FIDO 미지원 단말 사용자를 위해, 모바일 OTP, Push, SMS, PIN, Email로 인증 가능
			2차 인증을 위해, FIDO 인증을 2차 인증용으로 사용 가능
		모바일 환경	FIDO 인증을 위한 전용 APP 제공을 통해 서비스 APP과의 APP to APP 을 지원
			FIDO 기능을 지원하는 SDK 제공을 통해, In-APP 형태를 지원
		PC 환경	Window Hello 연동을 통한 PC 로그인 시, FIDO 인증을 지원
			Edge, Chrome 등 과 같이 W3C 표준을 지원하는 브라우저의 WebAuthn 인증 가능 (PC내 별도의 설치 없음)
			Push, QR 연동을 통한 스마트폰 인증과 PC 서비스 / 업무 환경의 인증 연계를 지원
			자체 개발한 CS용 lib를 직접 개발하여 CS환경까지도 모두 지원 (사내 메신저 등)
	Server	호환성	FIDO 표준 준수를 통해, 다양한 Authenticator와의 호환성을 제공함
		사용자 포털	사용자 본인이 직접 서비스별 인증장치(FIDO, CTAP, OTP 등) 등록 및 관리가 가능하도록 셀프 관리 기능 제공
		시스템 연동	서비스 연동을 위한 연동 규격을 제공
			RESTApi 지원을 통해 시스템 연동간 손쉬운 구축 환경을 제공
			LDAP, DB, EXCEL, AD 방식의 인사정보 연동 지원
			스케쥴러를 통항 인사정보 자동 업데이트 지원 (매일/매주/매월 및 연동 시간 설정 가능)
		관리기능	메타데이터, Facet ID 설정을 통한 접근 및 사용 가능한 인증 장치 통제 가능
			서비스별 관리자를 각각 설정하여 관리 가능
			사용자별 인증장치 등록 현황 및 사용자 전체 현황을 제공
			사용자별 인증 내역의 현황을 제공
			서비스별 사용 가능한 인증장치 관리 기능 지원
			FIDO 인증장치와 OTP의 통합 관리 기능을 제공
			서비스별 사용자 그룹 매핑을 통한 편리한 인증정책 관리
			메뉴 관리 – 인증 서비스 메뉴관리 및 메뉴별 허용 인증장치 관리
			미소지자 워크플로우 – 단말기 미소지 경우 관리자 승인을 통한 접근 프로세스 지원
		VPN 환경	VPN 접속을 위한 1,2차 인증을 지원
			VPN의 수정을 최소화하기 위해, Radius 프로토콜을 지원

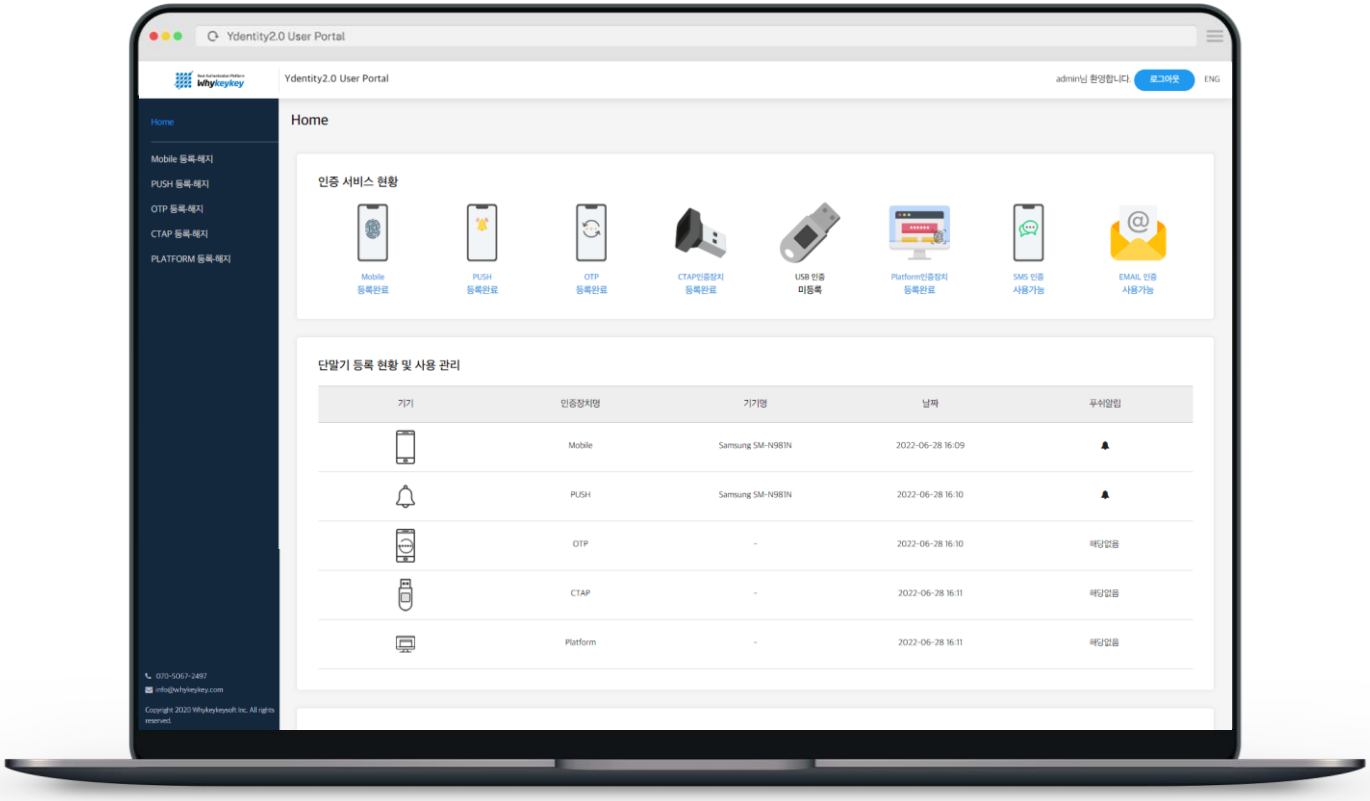
FIDO2 Admin Portal

관리자 포탈은 FIDO2 인증 사용과 관리를 위한 통합 정보 창을 통해 미등록자/등록된 장치별 현황/서버모니터링 등을 한 눈에 파악할 수 있도록 지원하고 있습니다.

1. 서비스별 분석이 용이하도록 통합 정보창 제공
2. 서비스별 전체 등록/미등록 사용자 확인 및 바로가기 조회
3. Mobile 생체인증/OTP/Push/CTAP /SMS/Email 등 등록된 인증수단 통합 관리 및 한눈에 파악
4. Ydentity서버의 CPU/메모리 실시간 모니터링
5. 서비스 연동을 위한 손쉬운 RESTApi 방식의 연동 지원

FIDO2 User Portal

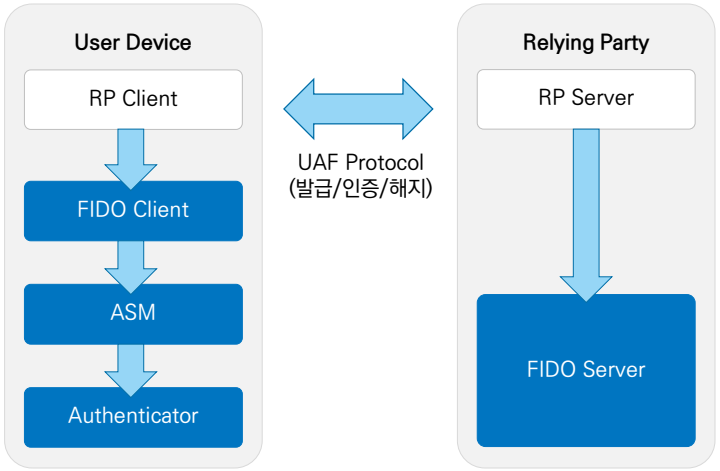
**사용자 포탈은 관리자가 설정한 권한 내에서 사용자가 쉽게 인증 등록할 수 있도록 하며,
본인의 인증 장치를 직접 관리함으로써 관리자 업무도 최소화되도록 합니다.**



1. 등록한 인증수단 파악을 위한 사용자별 통합정보 Home 지원
2. 서비스별 멀티 인증수단 등록 가능 (Mobile/Push/OTP/CTAP/Platform /SMS/Email)
3. 사용자가 필요에 따라 직접 인증수단 등록/조회/해지가 가능하도록 Selfservice지원
4. 초기 사용자의 경우 편리한 등록을 위한 설정 가이드 지원
5. 단말기 미소지 시 인증을 위한 일회성 보안링크 요청

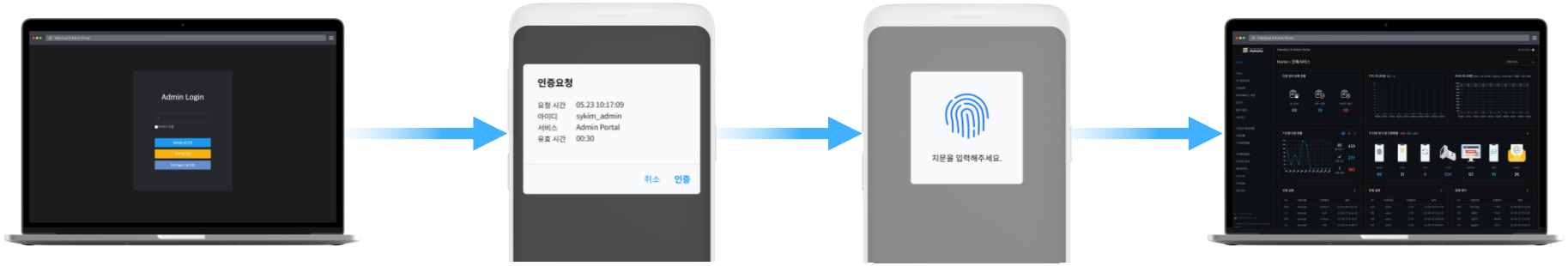
Mobile 생체인증 로그인 (FIDO2)

스마트폰을 통한 생체인증은 보안 강화를 위해 Password없이 ID만 입력 후 스마트폰에 기본 탑재된 다양한 생체인증장치(지문, Face ID 등) 기반으로 FIDO 인증 가능하도록 합니다.



FIDO는 비밀번호 없이 본인의 스마트 기기를 통한 인증 후 온라인 서비스를 이용할 수 있도록 합니다. 개인용 스마트 기기는 타인의 이용 가능성이 낮고 지문, 홍채, 안면(Face ID) 등의 첨단 바이오 인식 기술을 통해 간편하면서도 강도 높은 인증을 가능하게 합니다.

기본 사항으로 마켓 등록 정식앱 및 SDK 제공을 지원하며,
고객사 요건에 따라 추가 개발 지원을 통한 독립앱(In-App) 등
다양한 방식으로 Android/iOS 클라이언트를 제공이 가능합니다.



업무 로그인 | FIDO 인증 요청 Push | 모바일 FIDO 생체인증 | 로그인 완료

FIDO2 전용 인증장치(CTAP) 로그인

FIDO2 표준 인증을 지원하는 브라우저(Chrome, Edge, Safari, Firefox)와 Windows10에서 패스워드 없이 전용 인증장치를 이용해 인증할 수 있도록 지원합니다.

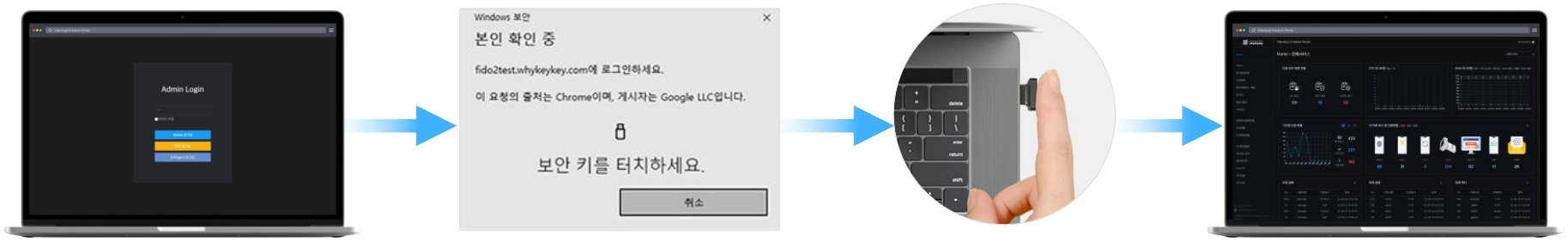
※ CTAP – 보안 키와 같은 외부 인증자가 USB, Bluetooth, NFC를 통해 강력한 인증 자격 증명을 사용자의 액세스 장치에 통신할 수 있게 하는 외부 인증장치 규격을 말합니다.

Supported In

W3C Web Authentication
An API for accessing Public Key

높은 인식률의 지문 센서와 보안 칩을 통한 생체정보 유출 차단되는 인증장치를 이용해 Password 입력 없이 One Touch만으로 빠르고 안전하게 로그인을 할 수 있습니다.

USB방식의 EzFinger2 전용 인증장치는 FIDO2 인증을 획득한 제품입니다.



업무 로그인 | CTAP 인증 요청 | CTAP 간편인증 | 로그인 완료

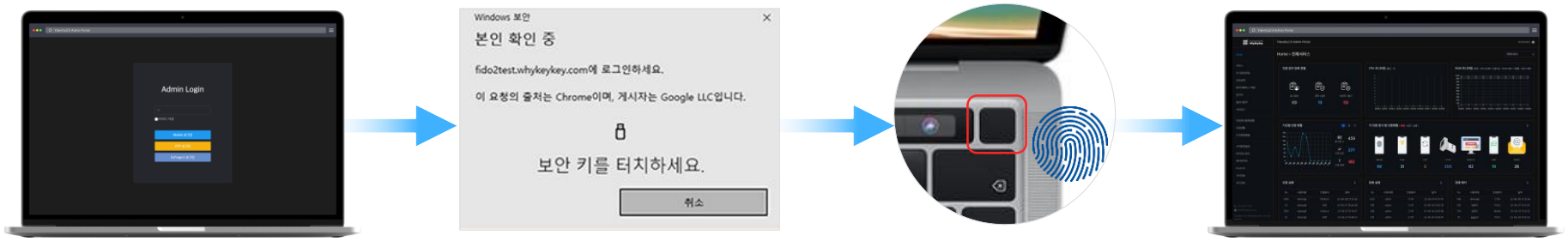
Platform 인증장치 로그인

Windows Hello와 macOs 기반 데스크탑 및 노트북에 내재되어 있는 장치를 활용하여 생체인증 로그인을 할 수 있도록 지원합니다.

보안강화를 위해 내재된 인증 장치 사용으로 쉽고 간편한 인증 지원!

삼성 및 맥북 등 최근에 출시되는 노트북 또는 데스크탑에는
기본으로 지문인식 센서가 탑재되어 있습니다.

별도의 인증장치나 모바일APP을 통해 로그인 하지 않고
내재되어 있는 지문인증장치를 통해 간편하게 로그인 할 수 있도록 지원합니다.

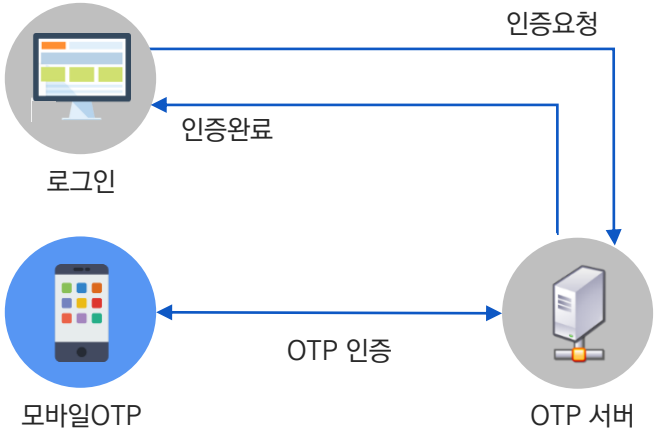


업무 로그인 | 지문 인증 요청 | 지문센서 간편인증 | 로그인 완료

Mobile OTP 로그인

인증 보안 강화를 위해 ID(Password) 입력 후 모바일OTP를 이용하여 추가 인증을 받을 수 있도록 하는 이중 보안 서비스입니다.

모바일 기반 OTP 기능을 제공하여 스마트폰을 사용한 OTP 인증을 수행합니다. 별도의 기기가 필요 없어 사용자의 편의성이 향상되며 Time Sync 방식의 OTP 생성으로 안전한 사용자 인증 기능을 제공합니다.

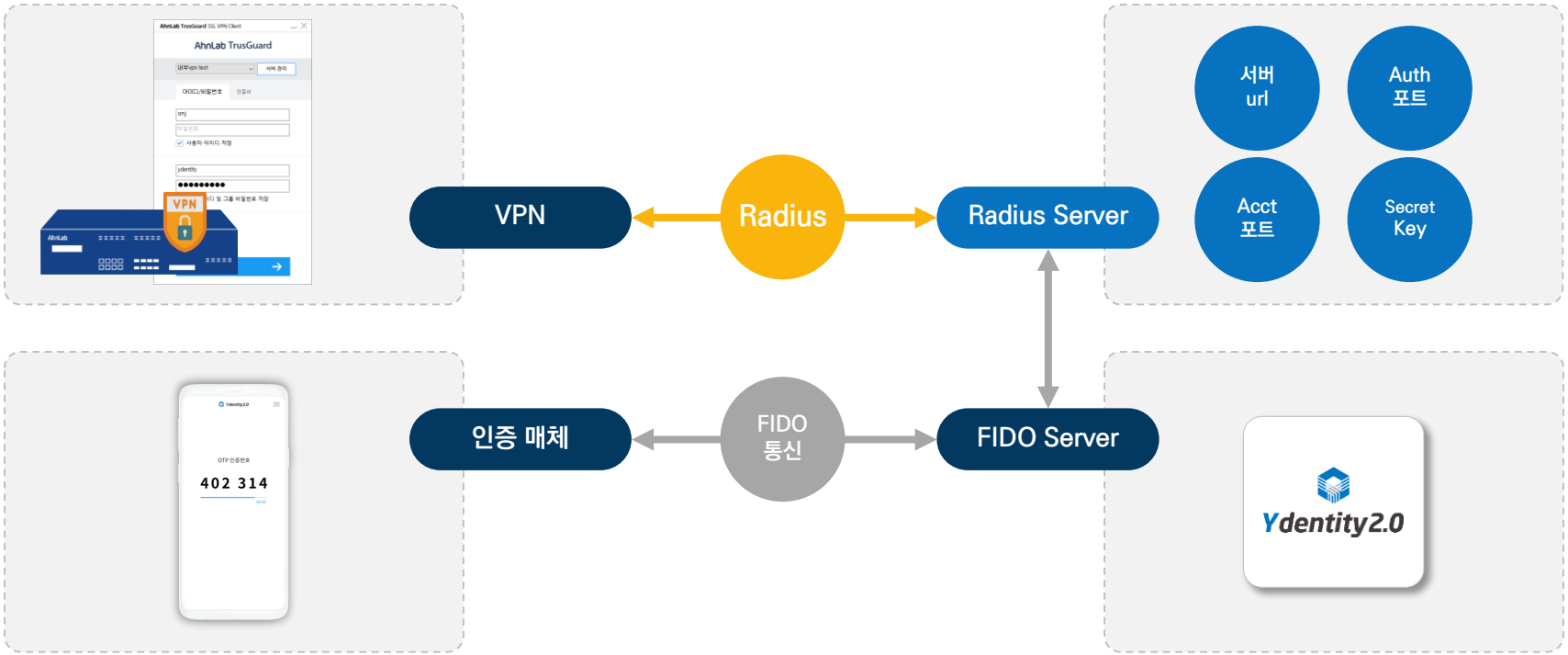


- 모바일 앱을 이용한 OTP 1차 / 추가 인증
- 별도의 기기없이 모바일 앱 설치로만 인증 수행
- Time Sync 방식의 안전한 인증

FIDO2 Radius Protocol

VPN에서도 별도 커스터마이징 없이 FIDO2 인증을 사용할 수 있도록 자체 Radius Protocol을 지원하여 생체인증 및 OTP 인증을 가능하게 합니다.

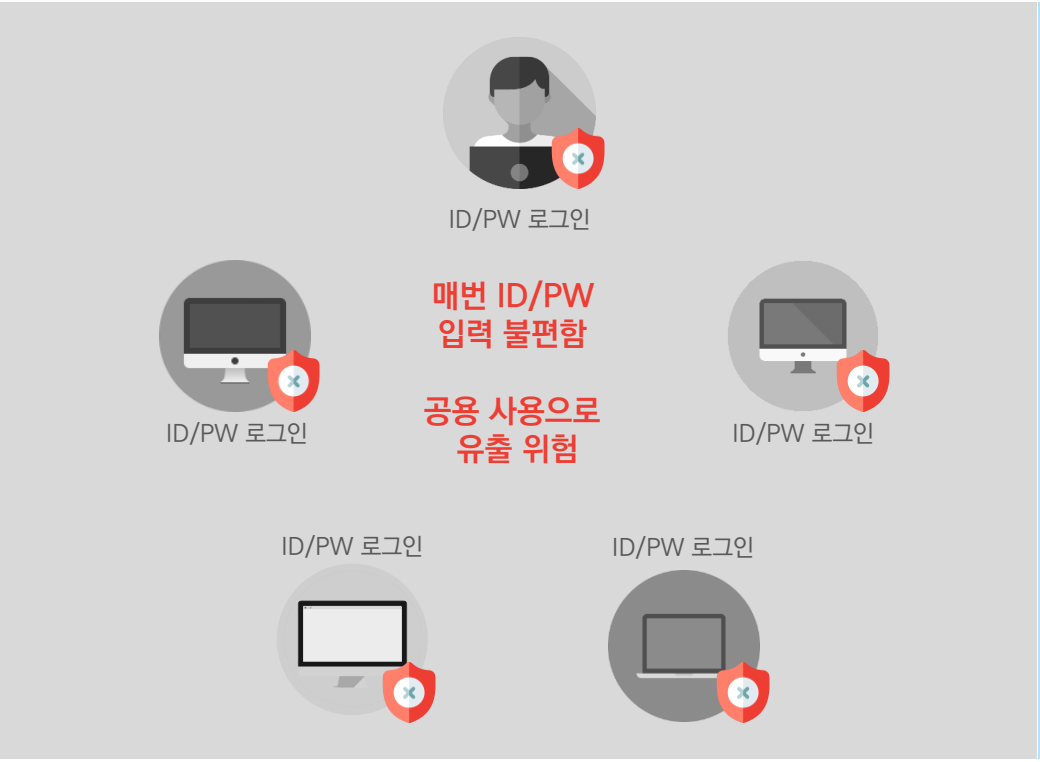
VPN 인증은 별도의 커스터마이징 없이 Ydeitnty2.0에 탑재된 Radius Server에 필요한 정보 설정을 등록하게 되고 이를 통해 FIDO Server와 통신하도록 미리 구현되어져 있어 해당 설정만으로 생체인증 및 OTP인증이 가능합니다.



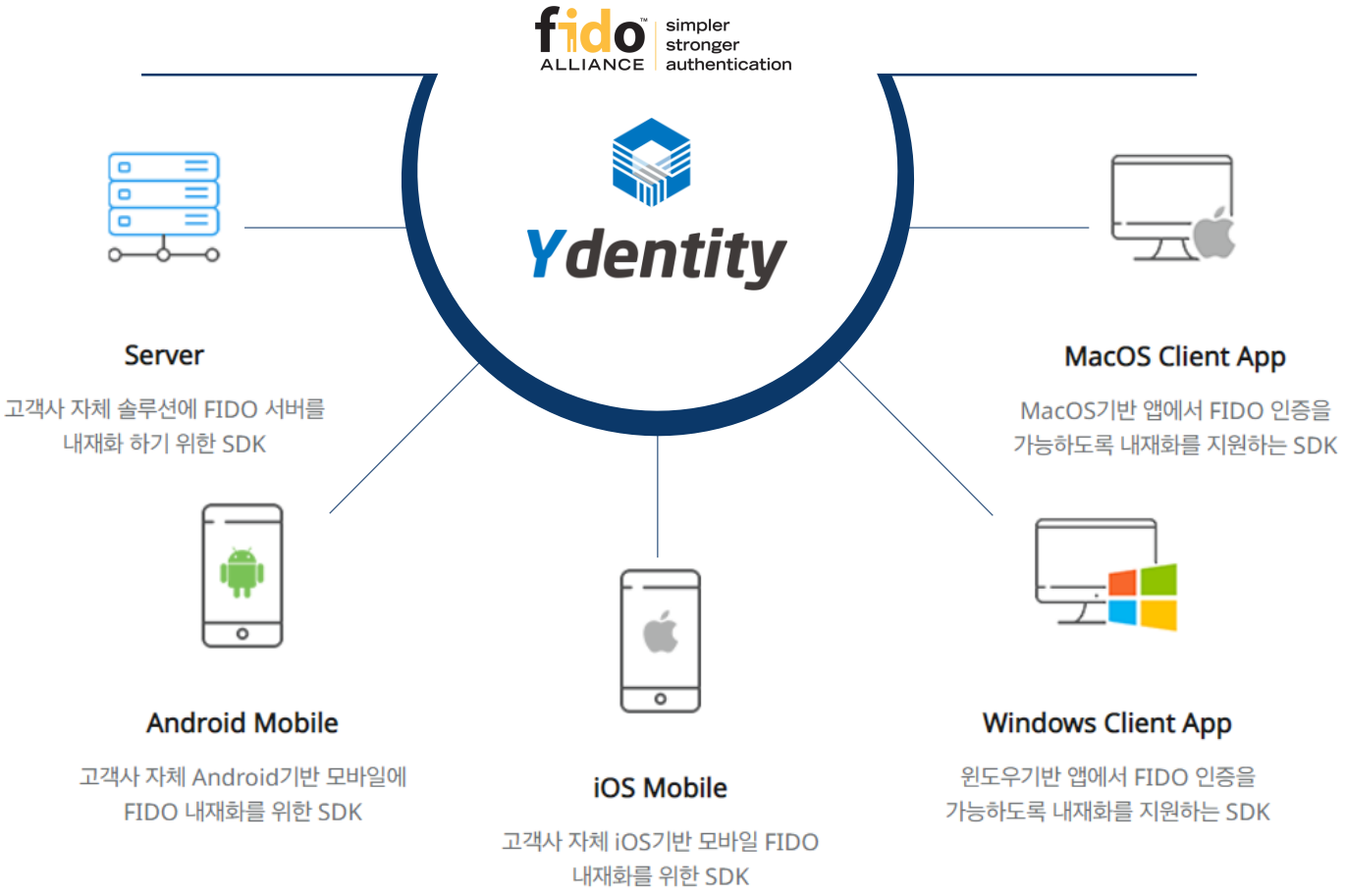
공용 인증장치 로그인

단 한번의 인증 등록으로 공용 인증장치가 있는 모든 곳에서 Password 뿐만아니라 ID 없이도 생체인증만으로 로그인을 할 수 있도록 구현합니다.

업무상 이동이 잦은 경우, 한 PC에서만 업무를 보지 않기 때문에 각 PC마다 로그인을 일일이 해야 하는 번거로움과 ID/PW 무단 공용 사용의 위험이 있습니다. 서버방식 공용 인증장치 로그인은 한번 등록으로 어느 PC에서라도 터치 한번 만으로 인증 처리가 가능하여 **업무 편리성과 개인 정보(ID/PW) 공유 차단으로 보안이 강화**됩니다.



Ydentity2.0 SDK – “고객사 제품에 lib, SDK 탑재 방식으로 진행!”



자체 브랜드로 영업

자체 솔루션으로 탑재
필요 시 고객사 명의로 FIDO
인증 획득 가능
획득 시 대외 영업 등
고객사의 FIDO2로 제안

AS 직접 운영

Lib, SDK를 제공함으로써
내부 정보 외부 유출
방지와 원활한 운영 및
유지보수 가능

04

솔루션 특징

04

신뢰성 – 인증 획득

FIDO Alliance의 FIDO 인증 획득을 통해 국제적 호환성이 검증되었을 뿐만 아니라, 국내에서는 GS인증 1등급 획득과 우수정보보호제품으로 지정되어 신뢰성과 보안성을 모두 갖추었습니다.

GS인증 1등급 획득

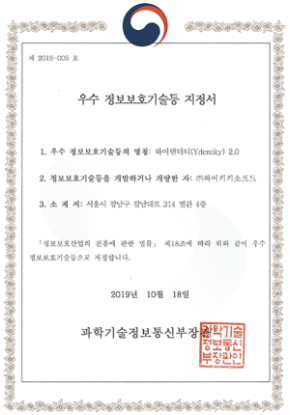
〈TTA – 2019〉

FIDO 1.0 및 FIDO2 인증 획득

〈FIDO Alliance – 2018〉

우수정보보호제품 지정

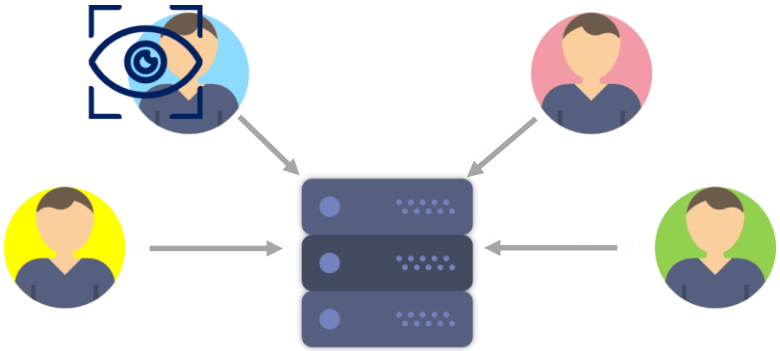
〈과학기술정보통신부 – 2019〉



보안성 – PKI 기반 인증 정보 분산화

사용자의 인증 정보를 보안에 취약한 서버에 저장하지 않아 **서버 해킹 위협으로부터 안전**하고
패스워드를 기억하지 않고도 다양한 인증지원으로 **편리하게 사용** 가능합니다.

서비스 제공자 집중형 인증 정보



인증 시 필요정보를 서버에 저장/관리

주요 해킹 목표, 해킹 시 2-3차 연쇄피해 발생

사용자에 분산화 된 인증정보

매체별·인증수단별 분산화 관리

사용자가 스스로 인증 핵심 요소를 보유·통제

Credential의 보관 및 사용기술 혁신을 통한 인증 패러다임의 변화

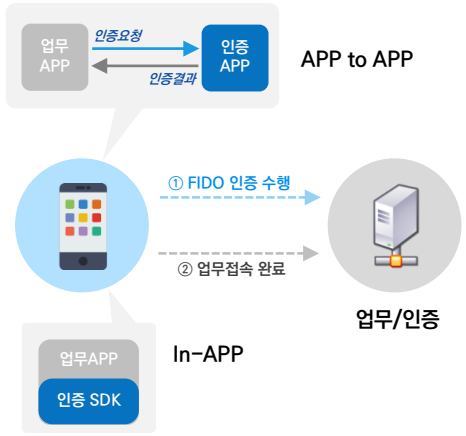
기술력 – 자체개발 기술력으로 다양한 인증환경 지원

Ydentity2.0은 PKI 및 FIDO 전문 개발 인력의 기술력으로 직접 자체 개발 하였기 때문에 다양한 인증환경 및 인증장치를 지원하는 것이 가능합니다.

구분		모바일 인증장치 연동	CTAP 인증장치 연동
모바일 환경	Android	인증 전용 APP 또는 In-APP (Embedded SDK)	-
	iOS	인증 전용 APP 또는 In-APP (Embedded SDK)	-
PC 로그인 (Windows로그인)	Windows 10	Universal APP 사용	Universal APP 사용
PC내 브라우저 환경		無설치 기반 연동	FIDO2 지원 브라우저 - 無설치기반 연동
PC내 C/S 환경		C/S내 SDK 배포	C/S내 SDK 배포

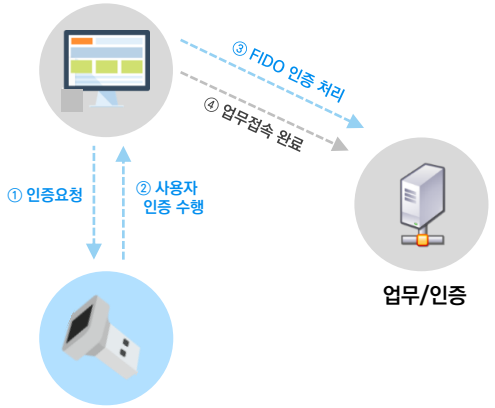
Push 또는 QR 연동

모바일 환경



PC 환경(모바일 인증장치 연동)

PC 환경(CTAP 인증장치 연동)



확장성 – 유연한 호환성으로 넓은 시장 확보

패스워드 대체뿐만 아니라 다양안 영역에서
사용자의 인증을 필요로 하는 모든 서비스에 적용이 가능한 초간편 인증 솔루션입니다.

B2C서비스 시장

- 서비스 인증
- 회원정보 수정
- 온라인 결제
- 계약체결(전자적 서명)

엔터프라이즈 시장

- 스마트오피스 및 PC로그인
- ERP 및 모든 업무 인증
- 전자결재 포함 그룹웨어 등
- VPN, SAC 인증
- 클라우드 접근(인증 전용 CASB)

05

도입 사례

05

주요 도입 사례

국내외의 FIDO2 인증, GS인증, 우수정보보호기술 지정 등으로 검증된 기술을 바탕으로 다수의 FIDO 인증 프로젝트를 수행하였습니다.

SK쉴더스 블루마스터 FIDO2 구축

양자암호기술을 이용한 FIDO 지문 보안키 적용
무인경비 보안관제 시스템인 블루마스터에
2차 인증 방식 적용

안랩 내부시스템 FIDO2 구축

내부 시스템에 와이덴터티 FIDO2 시스템 적용
레디우스 프로토콜을 이용한 VPN 인증 연동
LDAP을 통한 인사정보 연동

대전광역시 상수도사업본부 FIDO2 구축

수용가정보 시스템에
양자암호기술을 이용한 FIDO 지문 보안키 적용
카드형 지문인식 보안키 적용

푸르덴셜생명 스마트오피스 FIDO2 구축

내부 사용자를 위한 SSO와 스마트오피스 시스템에
와이덴터티 FIDO2 시스템 적용
LDAP을 통한 계정 연동

더존 그룹웨어 FIDO2 내재화 사업

와이덴터티 lib, SDK 제공으로
통합 그룹웨어와 ERP에 적용
웹브라우저, 메신저, 모바일앱에 FIDO2 적용

누리텔레콤 FIDO2 생체인증 구축

CTAP 인증장치를 이용한 FIDO 생체인식 구축

한국전자통신연구원 FIDO 개발

ETRI FIDO2 BLE 기술 개발

한국정보인증 전자서명 개발

무설치 HTML5 전자서명 개발 계약
PDF전자서명서비스/솔루션 용역 계약
공인인증서 솔루션 멀티 OS 개발

메가존 클라우드 기반 생체인증 개발

국제표준(FIDO) 방식의 사용자 인증
다양한 생체인증 확장을 위한 표준 프레임워크

바이오 정보 분산관리 시스템 구축(FIDO)

바이오 정보 분산관리 시스템 구축(FIDO)

안랩 – 국내 보안의 선도 안랩과 솔루션 제휴 및 내부 인증 구축

전략적 투자 진행

- 안랩 최초 인증기술 유망 스타트업 “와이키키소프트”에 대외 투자 진행
- 안랩 제품 내 와이키키소프트의 생체인증 기술 탑재
- 중소기업 상생 협력 모델 마련

내부 임직원용 인증시스템 구축

- 임직원을 위한 업무 시스템 및 VPN 로그인 시, 지문 기반의 간편인증
- RADIUS 프로토콜 지원을 통해, 기존 Legacy 환경의 영향 없이 적용

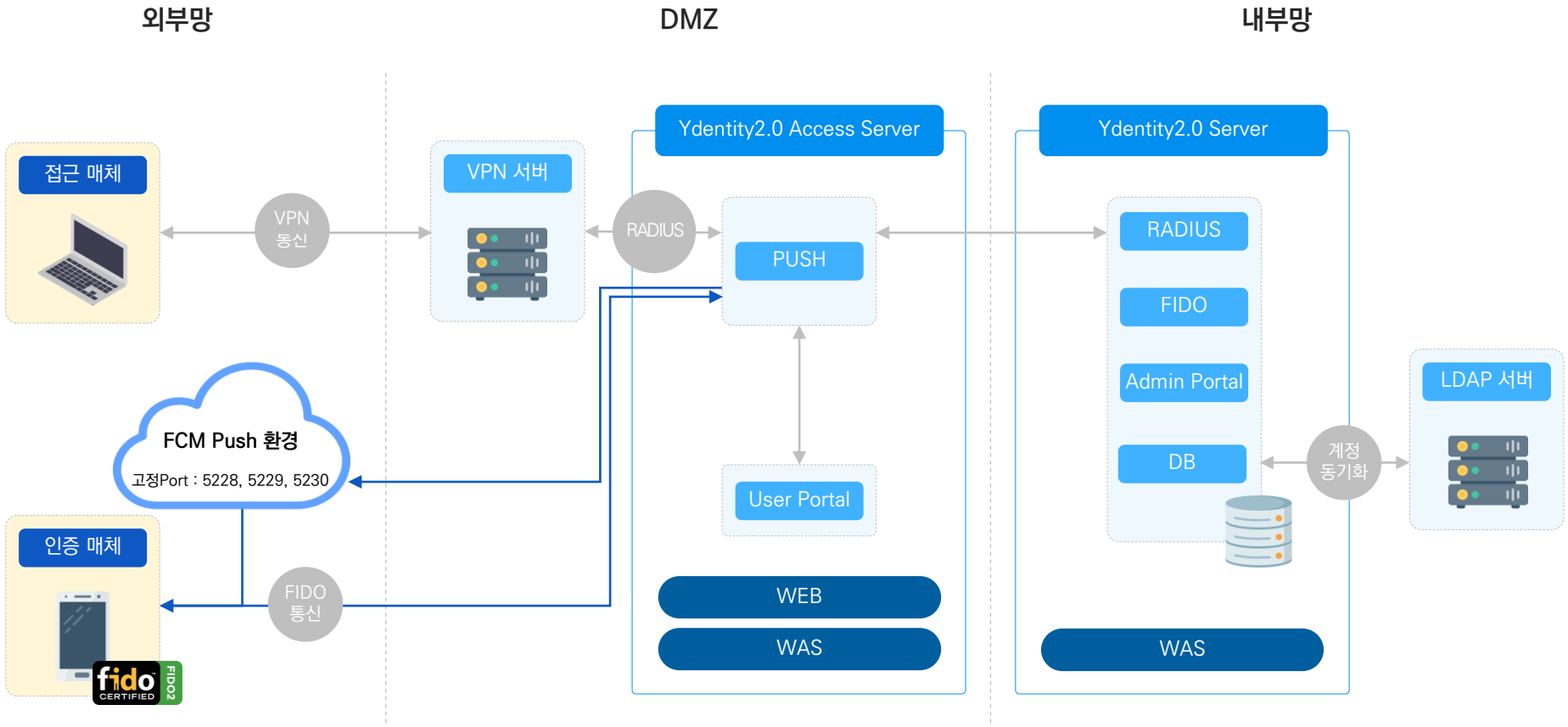
VPN 인증 강화를 위한 제품 결합

- VPN 고객사의 간편 인증 및 2차 추가 인증
- VPN 제품 내 기본 탑재를 통한 구축 용이, 비용 절감 효과

AhnLab TrusGuard

안랩 도입 사례

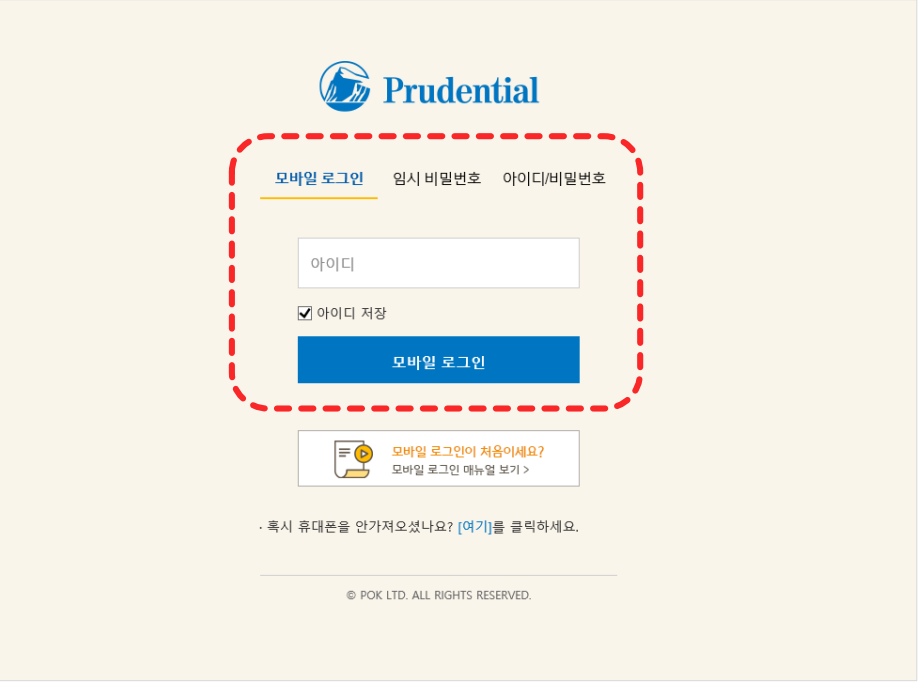
국내 보안의 선도 안랩과 솔루션 제휴 및 내부 인증 구축을 하였으며
LDAP를 통한 계정연동과 와이덴터티 자체 Radius를 이용하여 VPN 인증까지 적용한 사례입니다.



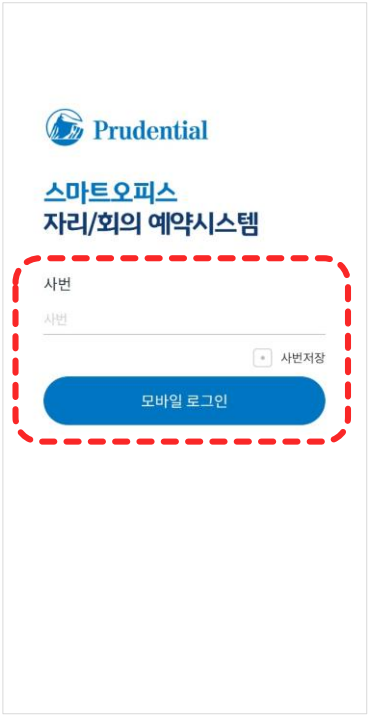
푸르덴셜생명 – 스마트오피스 시스템

푸르덴셜생명은 스마트오피스 시스템 구축 사업으로 Ydentity2.0 간편인증 솔루션을 도입하였으며, SSO와 좌석예약시스템에 연동하여 간편인증 로그인을 적용한 서비스 사례입니다.

푸르덴셜 SSO(PC)

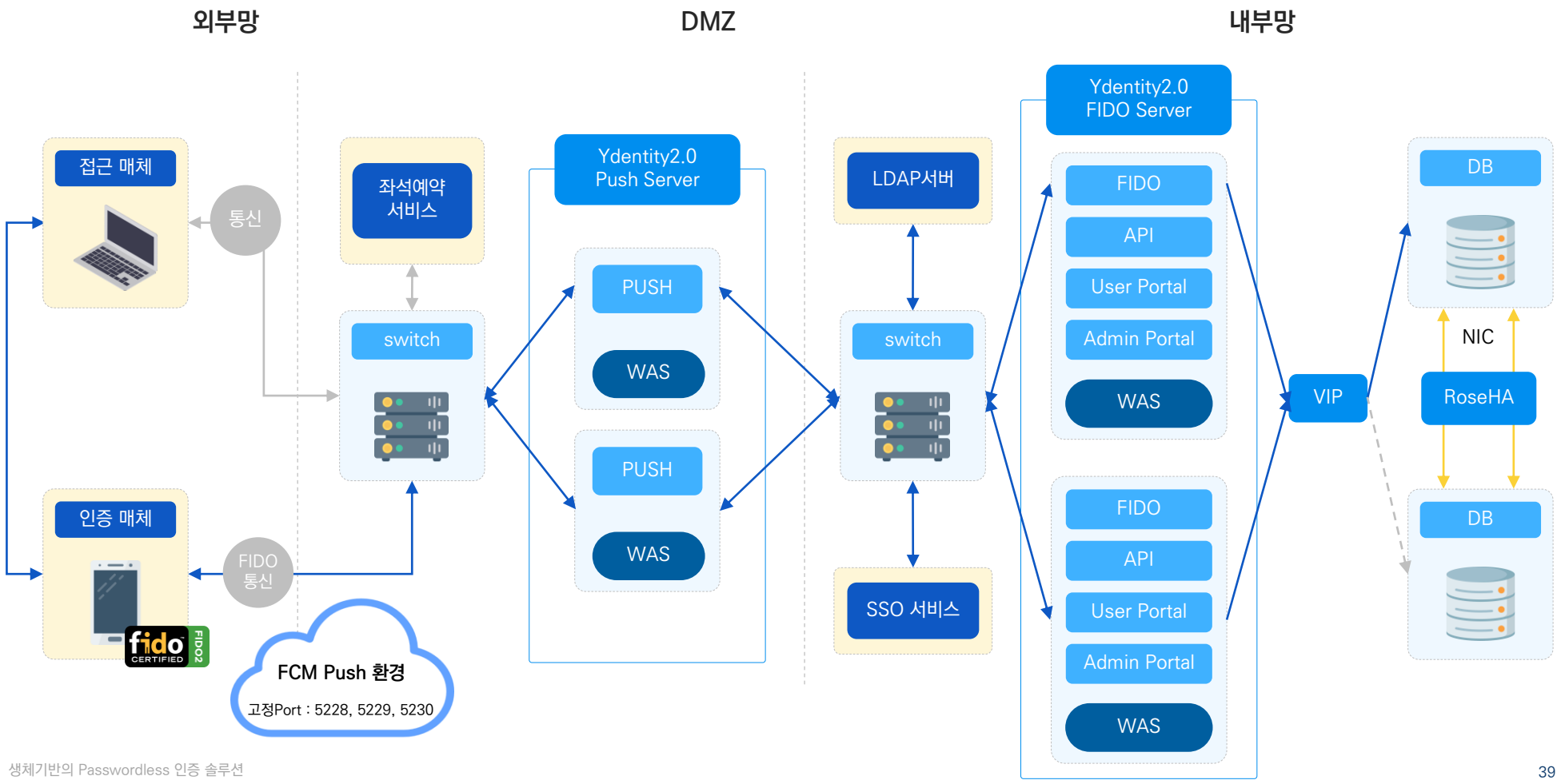


푸르덴셜 좌석예약시스템(Mobile)



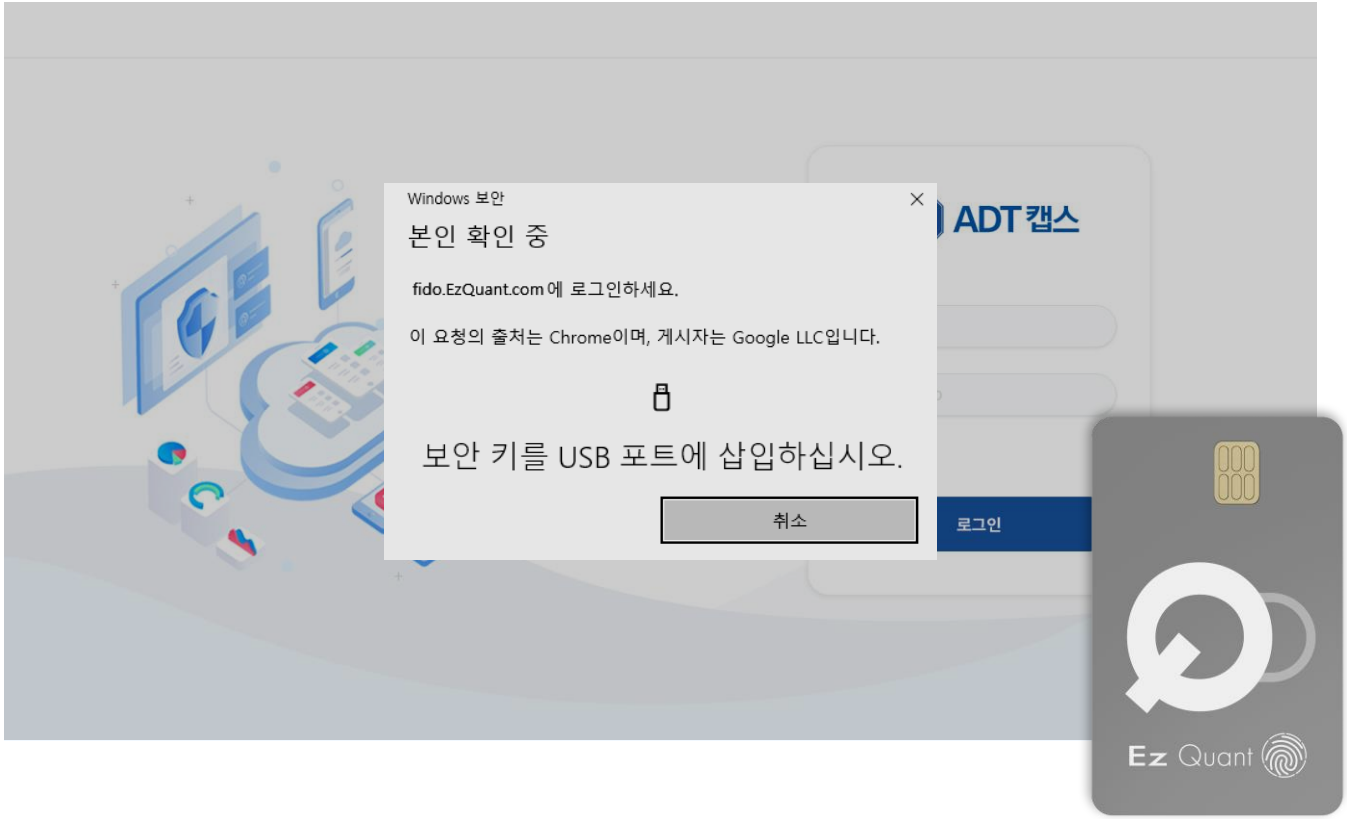
푸르덴셜생명 도입 사례

푸르덴셜생명의 내부 Ydentity2.0 FIDO 인증 솔루션 구축을 하였으며 LDAP을 통한 계정연동과 SSO, 좌석예약시스템 서비스를 연동하여 간편인증을 적용한 시스템 구성 사례입니다.



SK 쉴더스(ADT) - 무인경비 보안관제 시스템

SK 쉴더스(ADT)는 2021 양자암호통신 시범인프라 구축 · 운영사업으로 Ydentity2.0 FIDO 인증 솔루션 구축을 하였으며, 무인경비 보안관제 시스템인 블루마스터에 연동하여 2차 인증으로 적용한 사례입니다.



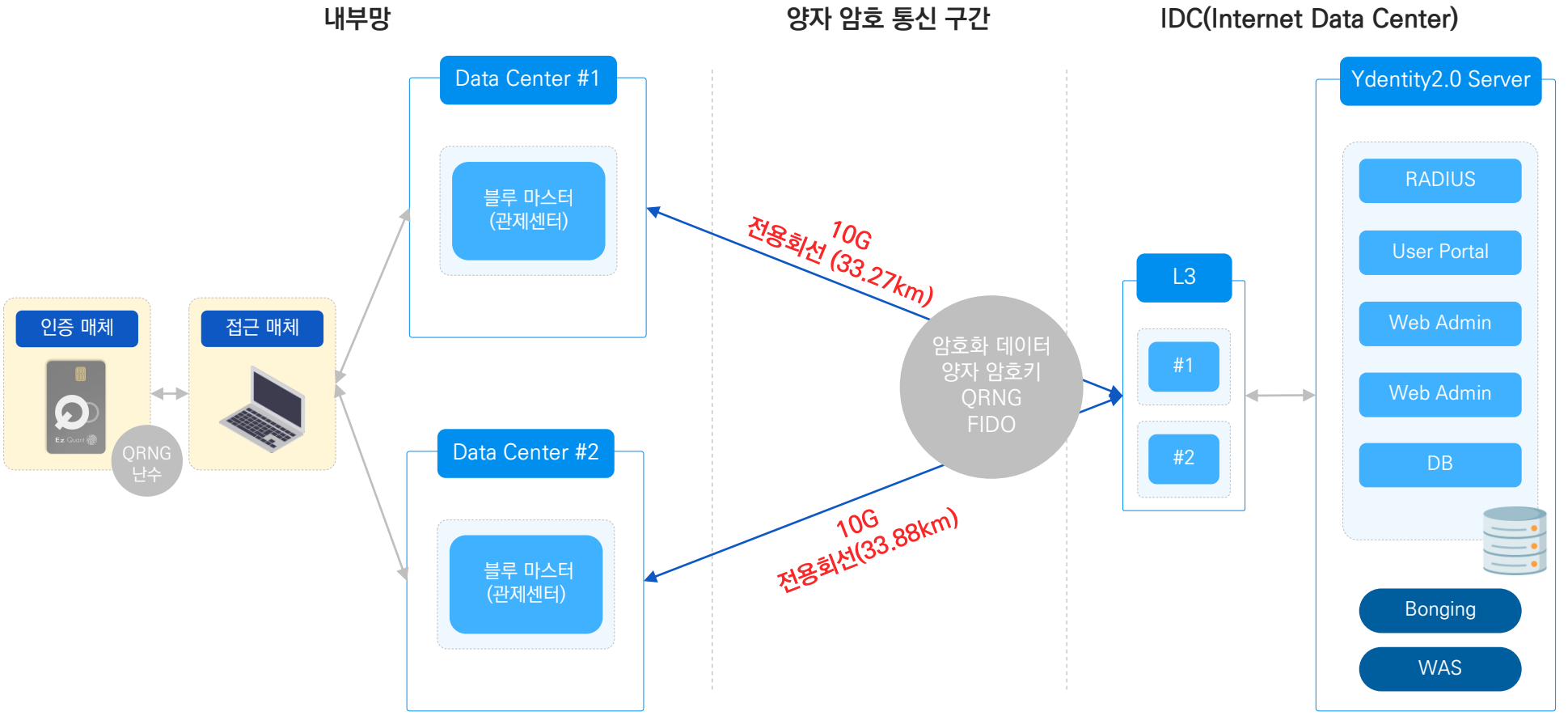
간편하고 강력한 양자암호

EzQuant 2차 인증

- 양자난수를 이용한 FIDO 지문 보안키
- 예측 불가능한 값을 암호화 키로 생성
- 어디서든 사용할 수 있는 간편함
- 물리적 인증과 온라인 인증을 한번에 가능
- 사용자를 정확하게 식별하는 지문 인식 기술
- USB타입 리더기를 통해 카드 인식 가능

SK 쉴더스(ADT) 도입 사례

SK 쉴더스의 내부 Ydentity2.0 인증 솔루션을 구축 하였으며, 데이터센터 2곳에 블루마스터 각각 연동하여 카드형태인 보안키로 인증할 수 있도록 적용 하였고, 양자 암호 전용통신라인을 설치한 시스템 구성 사례입니다.



대전광역시상수도사업본부 - 수용가 정보시스템

대전광역시상수도사업본부는 양자암호통신 시범인프라 구축 · 운영사업으로
Ydentity2.0 FIDO 인증 솔루션 구축을 하였으며, 수용가 정보시스템에 연동하여 2차 인증으로 적용한 사례입니다.

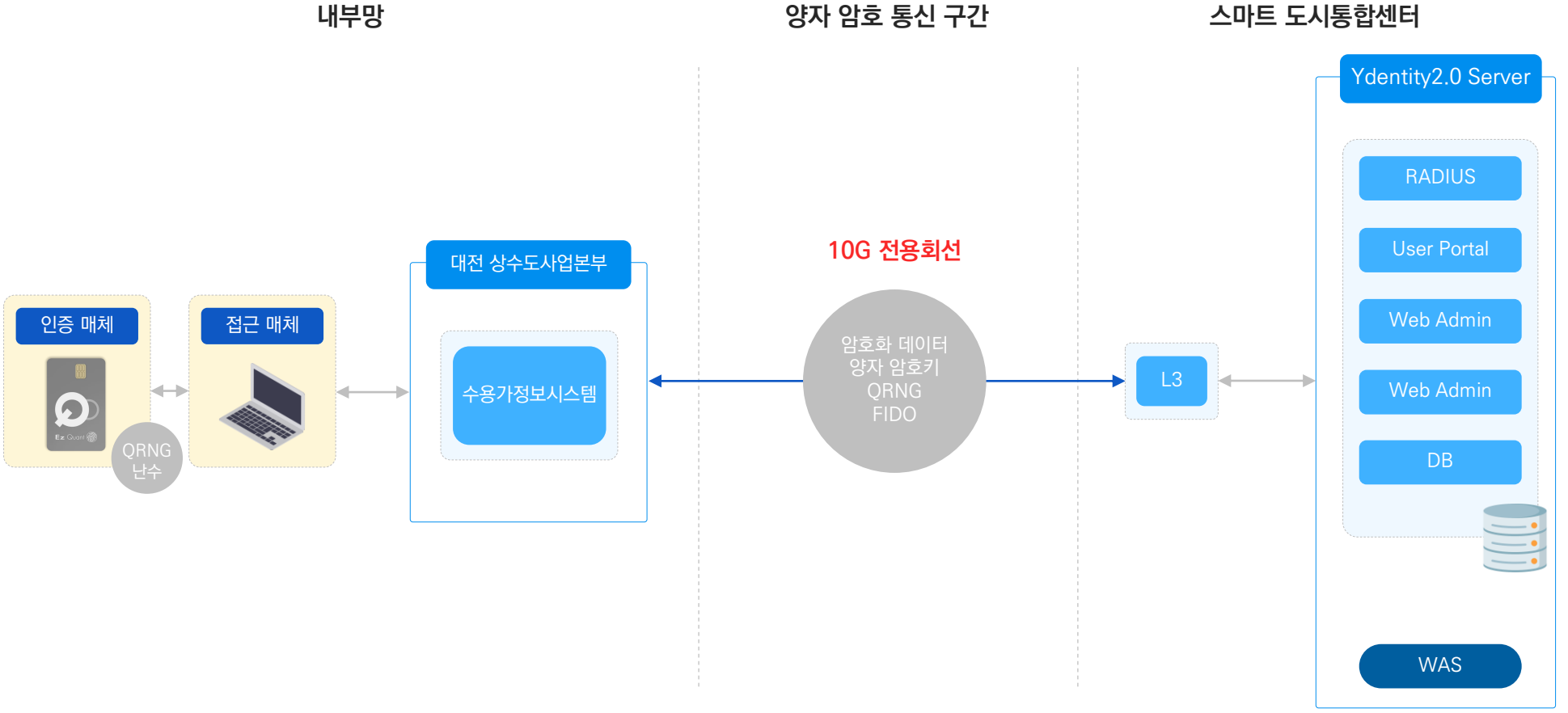
간편하고 강력한 양자암호

EzQuant 2차 인증

- 양자난수를 이용한 FIDO 지문 보안키
- 예측 불가능한 값을 암호화 키로 생성
- 어디서든 사용할 수 있는 간편함
- 물리적 인증과 온라인 인증을 한번에 가능
- 사용자를 정확하게 식별하는 지문 인식 기술
- USB타입 리더기를 통해 카드 인식 가능

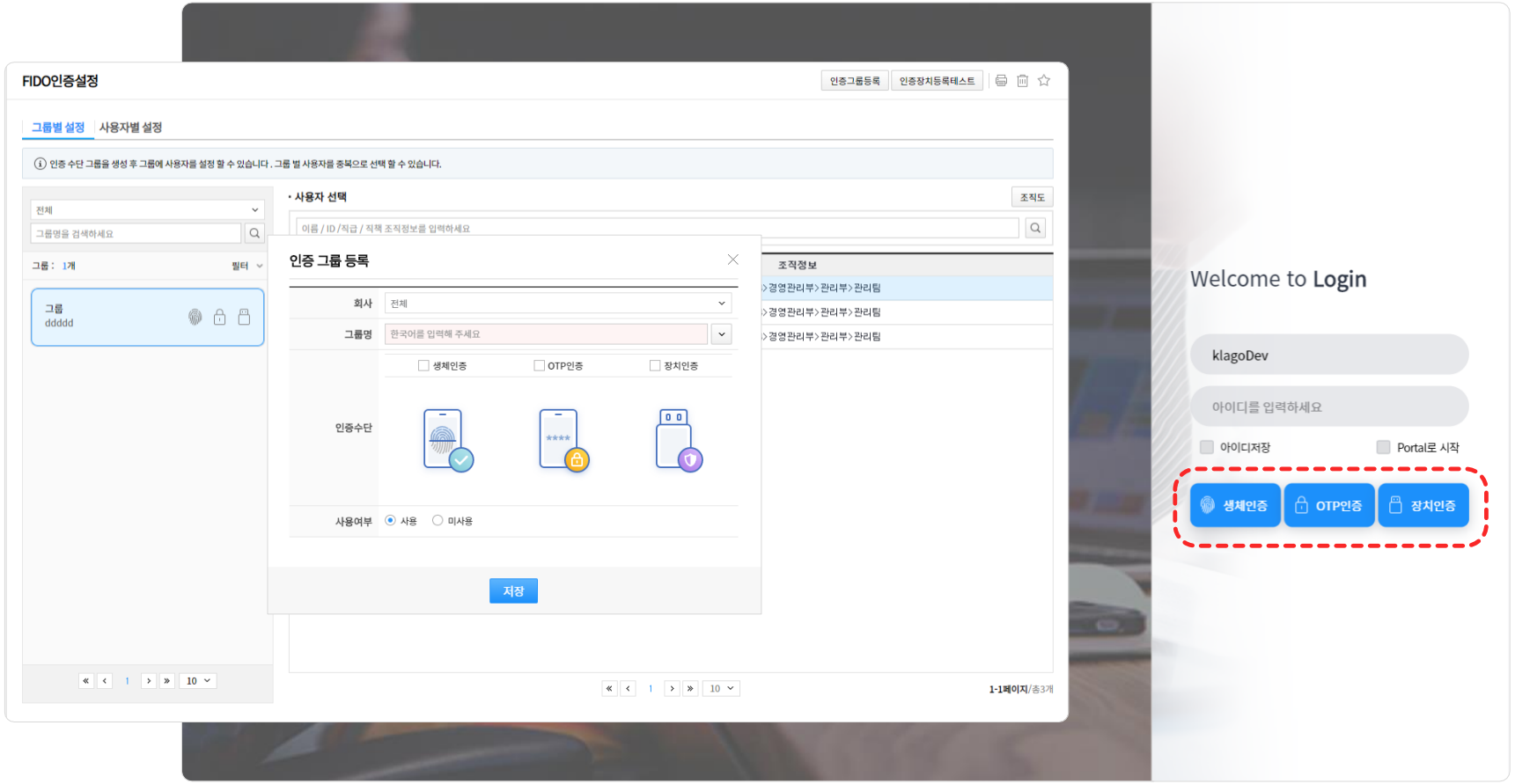
대전 상수도사업본부 도입 사례

대전광역시상수도사업본부의 수용가정보시스템에 Ydentity2.0 FIDO 인증 솔루션을 구축 하였으며,
양자 암호 전용통신구간으로 DATA를 보호하여 카드형태인 보안키로 인증할 수 있는 시스템 구성 사례입니다.



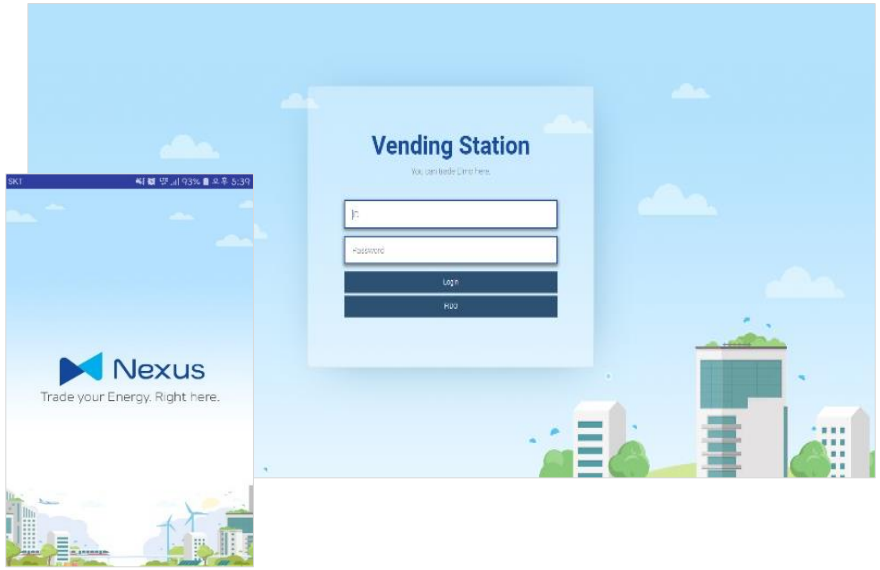
D 그룹사 도입 사례

Ydentity2.0 SDK 적용 사례로 국내 최다 고객을 보유하고 있는 D사의 그룹웨어(ERP) 솔루션에 와이덴터티의 SDK를 내재화 하여 적용한 사례입니다.



사용자 인증을 필요로 하는 다양한 서비스로서의 확대

아프리카 가나
전력거래용 가상화폐거래소



- 가상화폐 거래소의 가장 중요한 사용자 인증영역에 생체인증, PIN 기반의 Ydentity 솔루션 공급
- AWS(유럽) 기반 클라우드 환경을 통한 유연성 검증

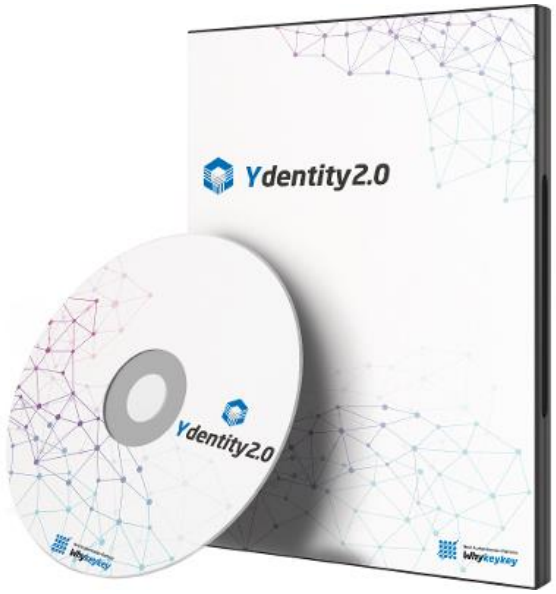
미래 지능형 자동차를 위한
차세대 인증기술 접목
(과학기술정보통신부 연구과제)

06

구축 및 유지보수

06

조달 등록 정보



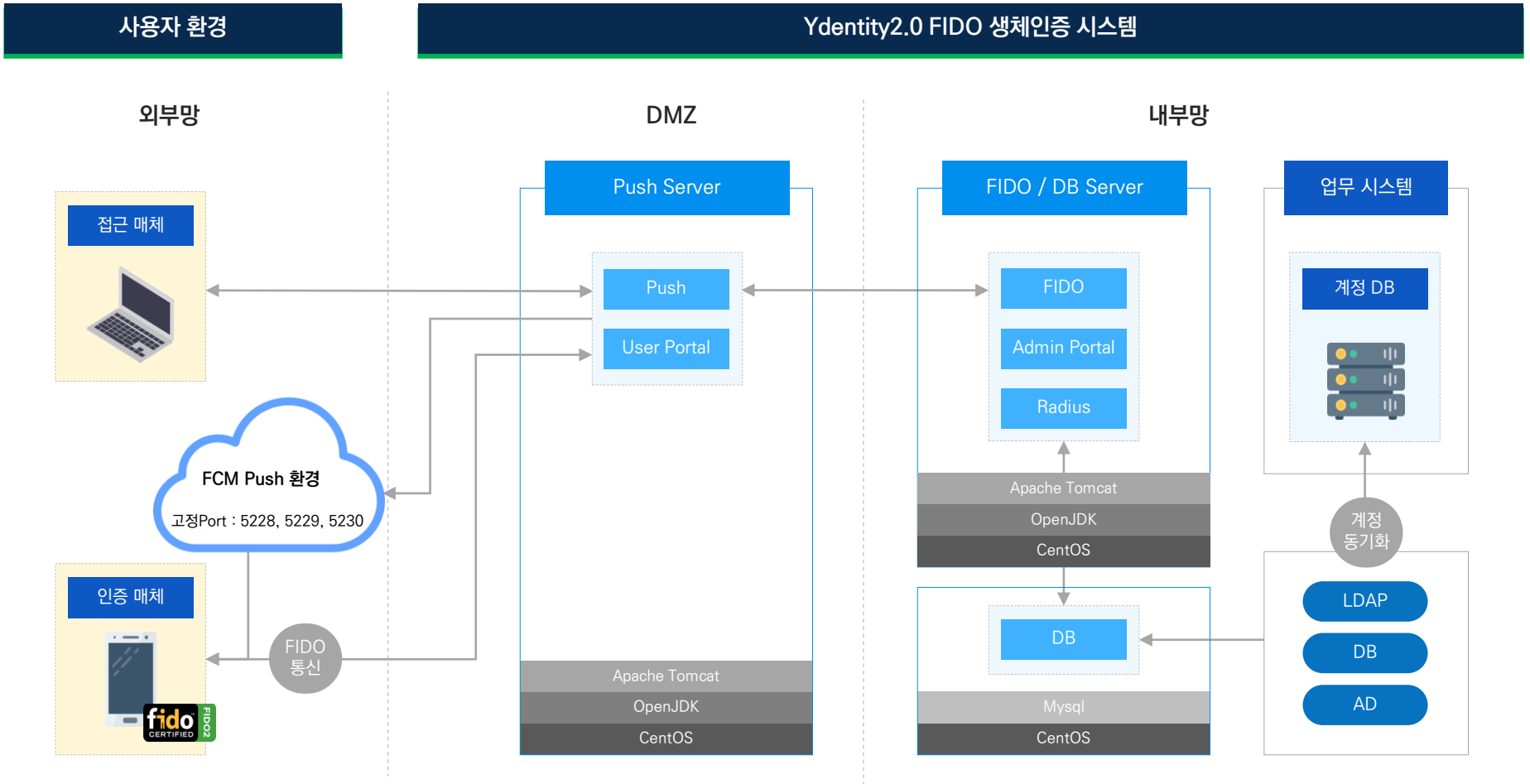
신뢰성과 보안성을 모두 갖춘 초간편 인증관리 소프트웨어

- FIDO Alliance의 FIDO1.0 및 FIDO2에 대한 상호호환성 테스트 완료 및 인증 획득
- ID/PW, 공인인증서 등에서 사용하는 로그인 방식 대신 생체정보, CTAP, mOTP 등을 이용한 사용자 간편인증 솔루션
- 모든 인증 Factor 및 연동시스템을 하나의 플랫폼 안에서 통합 관리 가능
- ERP, 인터넷 뱅킹, 간편결제, 게임, 포털, 전자결재, 그룹웨어 등 다양한 온라인 서비스와 본인인증 서비스에서 가능

분류	연동 라이센스	Client/iOS	Client/Android	FIDO 2.0 Server
물품목록번호	43231512-24350015	43231512-24350014	43231512-24350013	43231512-24346834
물품분류번호	43231512	43231512	43231512	43231512
물품식별번호	24350015	24350014	24350013	24346834
품목등록일	2021-09-02	2021-09-02	2021-09-02	2021-08-31
품명	인증관리시스템, 와이키키소프트, Ydentity v2.0, 연동 라이센스	인증관리시스템, 와이키키소프트, Ydentity v2.0, FIDO 2.0 Client/iOS	인증관리시스템, 와이키키소프트, Ydentity v2.0, FIDO 2.0 Client/Android	인증관리시스템, 와이키키소프트, Ydentity v2.0, FIDO 2.0 Server

시스템 구성도

Ydentity2.0은 Push Server / FIDO Server / DB Server로 구성되어 있으며, 구축 고객 정보에 따라 단일서버 또는 3대의 서버로 분리하여 시스템을 구성합니다.



시스템 사양

운영 환경

구분	분류	권장 사양
서버 환경	OS	centOS 7.0 이상 / Ubuntu 18.04 LTS 이상
	DB	MySQL 5.* 이상 / MariaDB 5.* 이상
	WAS	Apache Tomcat 9.0 이상
	Java 지원환경	Openjdk 11 이상 (무료) / Oracle java SE 8(1.8u202) 이상 (유료)
	SSL	금융결제원 SSL 등 (유료)
	브라우저	Edge, Chrome, Firefox 등 W3C를 지원하는 모든 브라우저
모바일 환경	Android	Android 6.0 이상
	iOS	iOS 10.0 이상
SDK	Android SDK	Android 6.0 이상
	iOS SDK	iOS 9.0 이상

서버 환경

구분	분류		권장 사양
서버 1대	단일 서버	CPU	Intel® Xeon® Gold 5220R 2.2GHz / 24Core 이상
		RAM	DDR 4 Reg ECC 64G 이상
		HDD	SSD 960G x 4 이상 Raid 1.0 구성
서버 3대	FIDO 서버	CPU	Intel® Xeon® Silver 4210 (10Core / 2.2GHz) 이상
		RAM	DDR 4 Reg ECC 8G 이상
		HDD	SSD 480G 이상
	Push 서버	CPU	Intel® Xeon® E-2334 (4Core / 3.4GHz) 이상
		RAM	DDR 4 Reg ECC 4G 이상
		HDD	SSD 480G 이상
	DB 서버	CPU	Intel® Xeon® Silver 4210 x 2 (20Core / 2.2GHz) 이상
		RAM	DDR4 Reg ECC 32G 이상
		HDD	SSD 960G x 4 Raid 1.0구성

[산정기준] 5,000명이 일일 각 10회 인증 및 한달 22일 기준으로 산정, 1건당 약 20MB, 1년당 약 250~300 GB 예상

구축 방법론

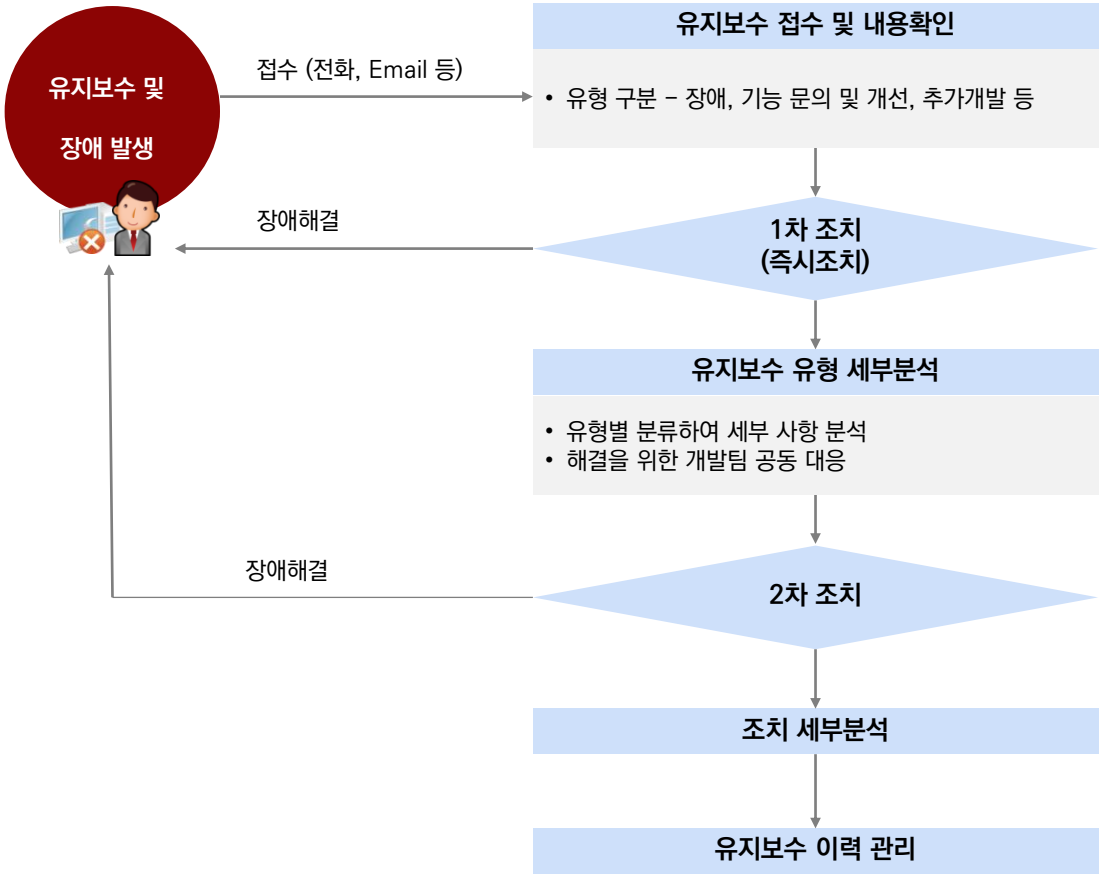
와이키키소프트는 사전 환경 분석으로 구축에 필요한 사항을 정확히 체크하고 체계적인 구축 Process를 통해 FIDO 기반 인증 시스템을 성공적으로 구축하고 있습니다.

단 계	세 부 내 용
KICK-OFF	• 계약사항 및 담당자 안내 • 구축 일정 협의 및 구축시 사전 필요 항목 안내
운영 환경 분석	• 시스템 환경 분석 (OS, DB, 이중화, 네트워크, 방화벽 설정 등)
연동 시스템 개발 협의	• 연동 시스템 개발을 위한 협의 및 API 제공
SW 설치	• Ydentity2.0 인증 시스템 설치 (서버, 모바일 등)
시스템 설정 및 교육	• 인사정보(LDAP, AD 등) 연동 및 SMTP, 인증정책 설정 • 운영을 위한 관리자 교육
연동 시스템 개발	• Ydentity2.0 로그인을 위한 페이지 수정 개발 진행 (적용 대상 시스템 개발사에서 개발 진행)
단위테스트	• 인사정보 연동 및 SMTP, 인증정책 적용 테스트 • Ydentity2.0과 연동 시스템 로그인 테스트
통합테스트	• 통합 테스트 • 시험 운영
운영	• Ydentity2.0 인증 시스템 실운영

유지보수 관리

무상 및 유상 유지보수 기간 내 발생하는 장애 상황에 대해 hot-Line을 통한 1차 즉시 조치 및 방문을 포함한 2차 조치를 통해 신속히 해결 해나가고 있습니다.

유지보수 대응 Process



1. 유지보수 접수

- 접수 : 고객사 → 유지보수지원팀
- 사전 장애 인지 시 고객사 담당자에게 우선 보고

2. 유지보수 1차 조치

- 바로 해결이 가능한 장애는 즉시 조치
- 유지보수지원팀 자체적으로 해결이 어려운 부분은 개발팀으로 통보하여 공동 대응
- 조치사항 관리와 유형 분석을 통한 유사 상황 대응

3. 유지보수 2차 조치

- 상황에 따른 개발팀 공동 대응 및 조치 진행
- 방문 조치가 필요한 상황 시 고객사 방문 대응
- 조치사항 기록 및 유형 분석

4. 접수 조치 결과보고

- 조치결과 보고

5. 유지보수 이력 관리

- 유지보수 결과 이력관리

07

와이키키소프트 소개

07

와이키키소프트는 초연결사회의 새로운 인증 패러다임을 열겠습니다.

와이키키소프트는 스타트업의 자세로 임직원 간의 신뢰와 도전을 통해 국내 및 글로벌 표준의 솔루션과 서비스를 공급하기 위해 노력하고 있습니다.
FIDO2기반 사용자 인증 솔루션 Ydentity2.0의 출시와 함께 우수 정보보호제품에 선정, GS인증 1등급을 획득하면서 국내 시장 공급을 시작하였으며
글로벌 진출을 바탕으로 패스워드가 없는 세상을 만들기 위한 와이키키소프트 임직원의 노력은 계속됩니다.

회 사 명 (주)와이키키소프트

설 립 일 2015.09.11

대 표 자 조한구

주요제품 Ydentity2.0(와이덴터티2.0)

회사주소 서울시 강남구 테헤란로87길 57 감령빌딩 5층 (06166)

인력현황 21명(2022년 3월 기준)

Next Authentication Platform
Whykeykey

고객사 및 협력사

다양한 기업과 고객관계를 유지, 협력하고 있습니다.

주요 고객사

금융결제원 Korea Financial Telecommunications & Clearings Institute
koscom
KICA 한국정보인증
한화테크윈
브이피(주)
Prudential
ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute
SK 쉴더스
대전광역시상수도사업본부
nuri TELECOM

협력사

DOUZONE
AhnLab
OCTATCO
NAON
Korea Digital Forensic Center 한국디지털포렌식센터(주)
NURIER SYSTEM
ITCREW (주)아이티크루
OWL 시아울시스템즈
STEALIEN we STEAL ALIEN technology
mobile C&C

연혁

2022

01 푸르덴셜생명 유상 유지보수 계약

한국정보인증 보안솔루션 유상 유지보수 계약

2021

12 대전상수도사업본부 수용가정보시스템 FIDO2 Ydentity2.0 구축

SK쉴더스(ADT) 블루마스터 FIDO2 Ydentity2.0 구축

11 사회연대은행 보안솔루션 유상 유지보수 계약

09 나라장터 국가종합전자조달 Ydentity2.0 등록

01 푸르덴셜생명 사내시스템 FIDO2 Ydentity2.0 구축

2020

12 D 그룹웨어 FIDO2 적용

11 안랩 사내 시스템 FIDO2 Ydentity2.0 구축

정보통신방송사업 우수성과 기업 선정

09 VP 안티스미싱서비스 개발공급 계약

누리텔레콤 FIDO2.0 업그레이드 계약

08 한국정보인증 보안솔루션 공급 계약

사회연대은행 보안솔루션 공급 계약

07 KB증권 축약서명솔루션 개발 계약

과학기술인공제회 보안솔루션 계약

2019

10 KSM (KRX Startup Market) 등록

Ydentity 2.0 제품 출시

과학기술정보통신부 – 우수정보보호제품 선정

TTA – GS 1등급 인증 획득

신용보증기금 “퍼스트 펭귄” 선정

03 안랩과 차세대 인증보안을 위한 업무협약 및 투자 유치

2018

10 K사, P사 FIDO2 서버 솔루션 공급

Ydentity 서버 및 인증장치 FIDO2 인증 획득

03 ETRI FIDO2 BLE 기술개발 계약

한국 FIDO 산업포럼 기술분과위원 및 컨설팅서비스 협력 계약

2017

10 AWS기반 바이오 인증서비스

06 정보통신산업진흥(NIPA) K-Global Startup 선정

05 국민대학교 창업선도대학 K-Startup 선정 및 최우수 졸업

04 한국인터넷진흥원(KISA) K-Global Security Startup 선정

2016

10 한국정보인증㈜ 공인인증서 솔루션 멀티 OS 개발 계약

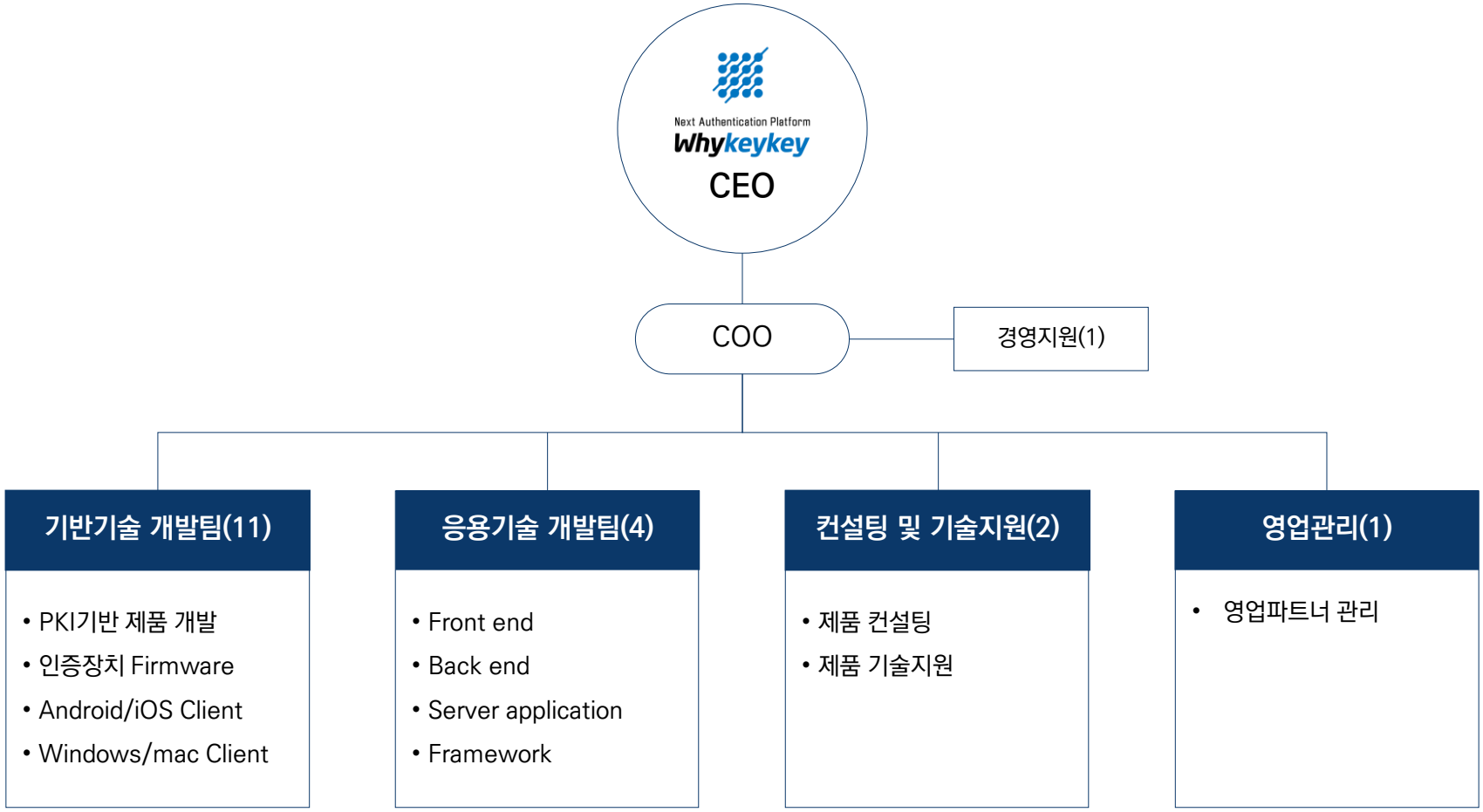
금융결제원 바이오 정보 분산관리 시스템 구축(FIDO)

2015

09 와이키키소프트 설립

조직도

- 70%의 인력이 개발/컨설팅/제품 엔지니어로 구성된 기술집약적 조직 체계
- 보안 및 인증영역 관련 10~20년 경력의 다수 보안 전문 인력으로 구성
- Firmware 및 USIM applet 전문 개발자를 통해 디바이스 인증에 대해 차별화된 경쟁력 보유



THANK YOU

Next Authentication Platform
Whykeykey

A. 서울시 강남구 테헤란로 87길 57 감령빌딩 5층(06166)

T. 02-576-4746

F. 02-578-4745

W. www.whykeykey.com