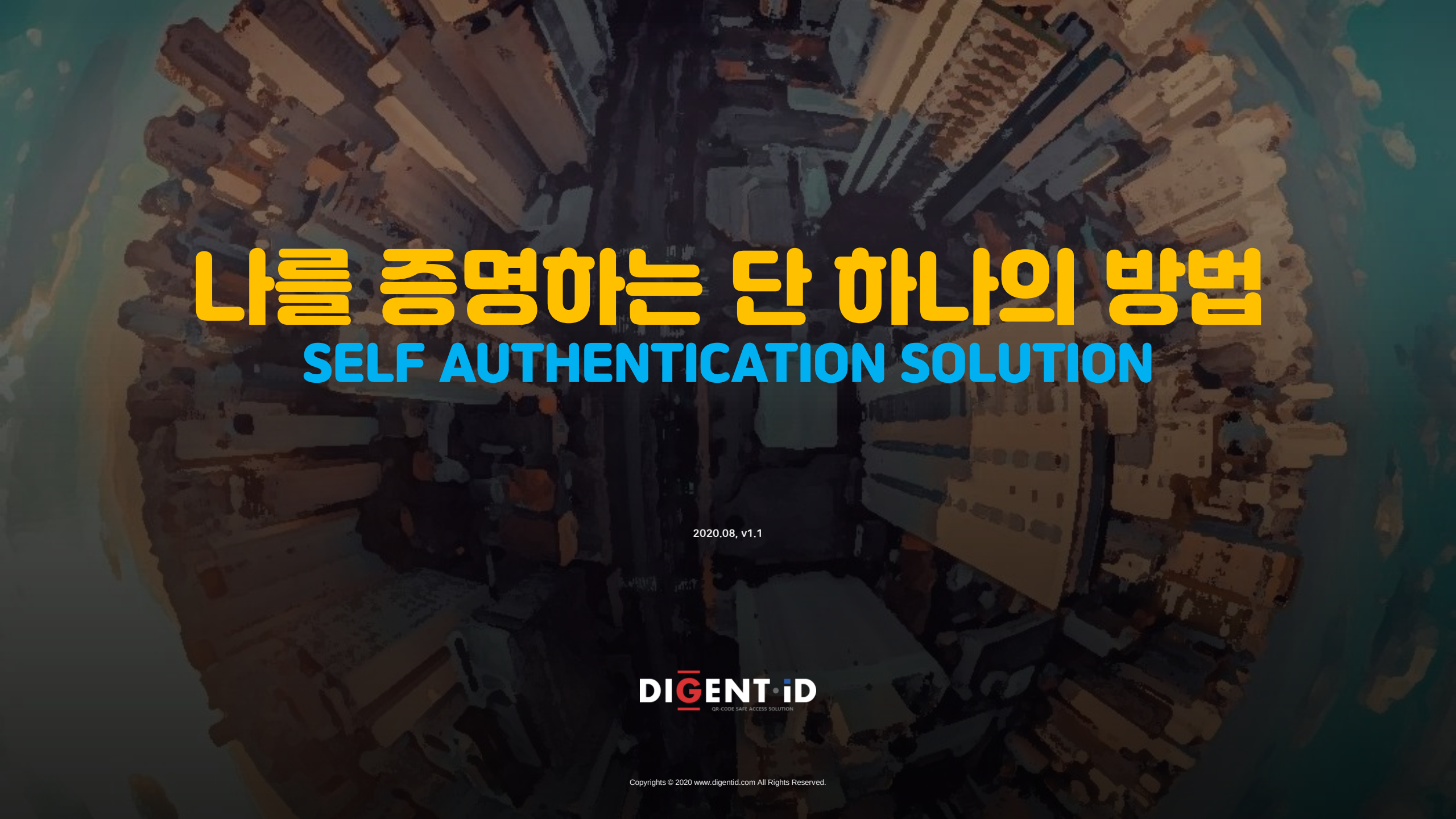


나를 증명하는 단 하나의 방법

SELF AUTHENTICATION SOLUTION

2020.08, v1.1

DIGENT·iD

QR-CODE SAFE ACCESS SOLUTION

목차

01

왜 iD·One이 필요한가?

개인인증의 어려움

DIGENT iD

01-1

왜 iD·One이 필요한가?

개인인증의 딜레마

PC 인증서 쓸려면…
보안 프로그램 깔고…
개인정보 등록하고…
휴대폰 본인 인증하고…
비밀번호 설정하고…
다 되었다…

근데 다른 곳에서 또 반복!…

VS

모바일 인증서 쓸려면…
모바일 어플 깔고…
개인정보 등록하고…
휴대폰 본인 인증하고…
PIN 설정하고…
다 되었다…

이거 하나면 정말 끝?…

01-2

왜 iD·One이 필요한가?

개인인증의 고민을 좀 더 자세히 보면

PC 인증서

↓

각종 보안 프로그램… 깔고

↓

또 계속된 반복…

VS

모바일 인증서

↓

전용 어플리케이션… 깔고

↓

또 호환이 안돼…

이 두가지가 고민이 다른 것 같지만 한가지 근본 원인이 존재한다.

01-3

왜 iD·One이 필요한가?

공인된 제3자의 중앙서버에 있는 개인정보로 인증하는 방식이 문제

기존의 인증방식

문제는 제3자의 중앙서버에 저장된 자신의 개인정보를 확인하는 인증방식

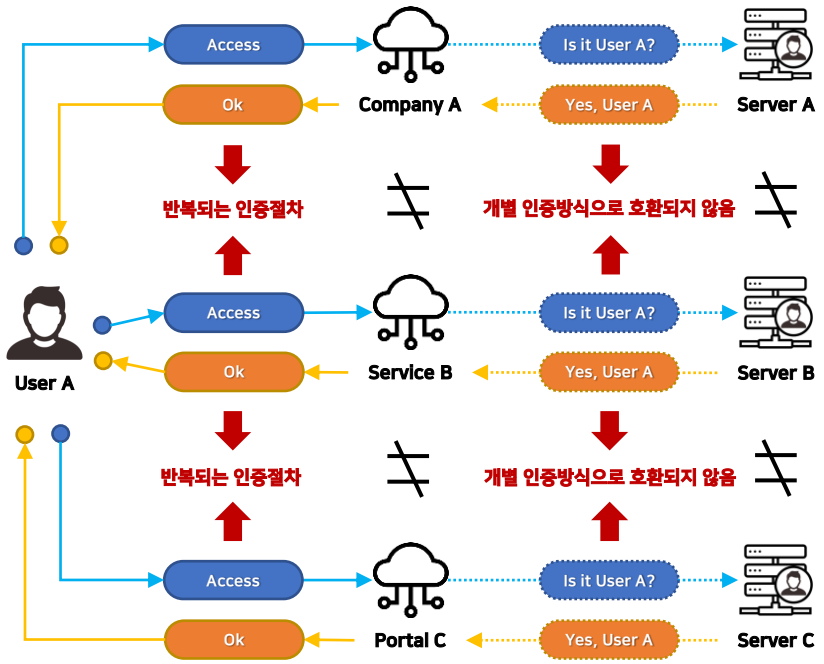
- 기존의 대표적인 인증방법: 공인인증서(공인기업), 아이핀(정부기관), 휴대폰 본인인증(이동통신사), 신용카드인증(카드사)
- 제3자에게 제공한 본인의 개인정보를 확인 받는 방식
- 기본은 여전히 아이디와 패스워드로 잊기 쉬움
- 개인정보가 제3자에게 있어 개인이 관리하기 어려움
- 제3자의 중앙서버와 자신의 단말기(PC/모바일 기기)에 개인정보가 존재해 항상 해킹의 위험성이 있음
- 다른 서비스나 플랫폼 간에 호환되지 않음

01-4

왜 iD·One이 필요한가?

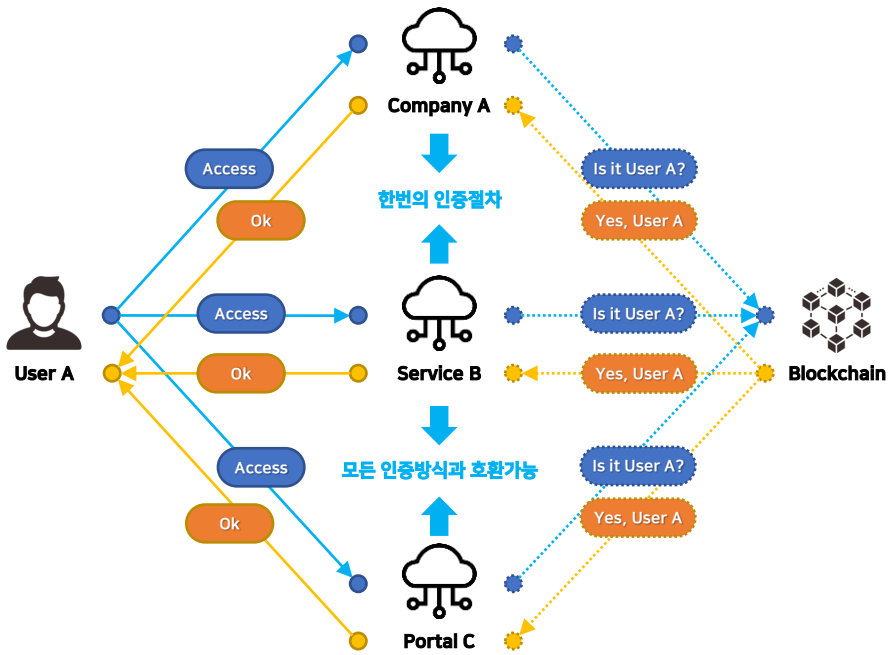
그래서 개인정보의 탈중앙화 된 인증방식이 필요함

제3자 인증을 통한 개별 인증 솔루션



TO BE

자가 인증을 통한 통합 인증 솔루션



우리의 소중한 개인정보 보호 및 편리함을 위해 iD·One 자가인증 솔루션을 추천

iD·One의 제안

자가 인증 솔루션

실제 생체인식 정보와 멀티 블록체인을 활용한
해킹의 위험에서 안전하고 자신의 개인정보를
자신이 관리하는 자가 인증 플랫폼

01-6

왜 iD·One이 필요한가?

iD·One 도입효과

- 통합 인증 솔루션을 통해 고객은 하나의 ID로 모든 온라인 서비스를 이용
  → **개인인증이 필요한 모든 부분을 하나로 통합**
- 비밀번호 없이 생체인식(지문 및 얼굴)을 통한 이용
  → **비밀번호 분실 위험이 없고 사용하기 쉬움**
- 개인정보는 이중 암호화되어 멀티 블록체인에 저장
  → **퍼블릭, 프라이빗 블록체인 이용, 해킹 위험 없음**
- 고객의 정보를 저장하고 보호하기 위해 중앙 서버가 필요하지 않고 오픈API로 어떤 시스템이든 쉽게 적용
  → **기업의 해킹 방지 및 보안 솔루션 비용 절감**
- 온라인과 오프라인 모두 사용가능
  → **디지털 신원 인증을 위한 우수한 플랫폼**

01-7

왜 iD·One이 필요한가?

이미 진행중인 통합 ID 서비스

- 자신의 소셜 로그인 계정을 바탕으로 이용자가 인터넷에서 다른 인터넷 서비스에 새로운 계정을 만들거나 계정에 접속하는 통합 ID 서비스
- 대표적인 소셜 로그인 서비스는 네이버, 카카오, 페이스북, 구글 등

행정안전부

하나의 아이디로 디지털원패스

- 행정안정부의 디지털 원패스는 하나의 아이디로 온라인 공공서비스를 간편하고 안전하게 로그인이 가능한 공공기관용 통합 ID 서비스
- https://www.onepass.go.kr/

02

iD·One이 뭐 길래?

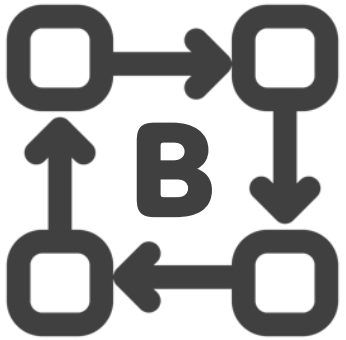
개인 인증에 꼭 필요한 iD·One 강점 3가지

DIGENT·iD

02-1

iD·One이 뭐 길래?

개인 인증에 꼭 필요한 iD·One 강점 3가지



멀티 블록체인

퍼블릭 & 프라이빗
블록체인 지원

리얼 생체정보

실제 지문과 얼굴의
인식정보 활용

오픈API 연동

다양한 플랫폼에
서비스 연동

완벽한 개인정보 보호 및 편리함을 최우선으로 하는 시스템

02-2

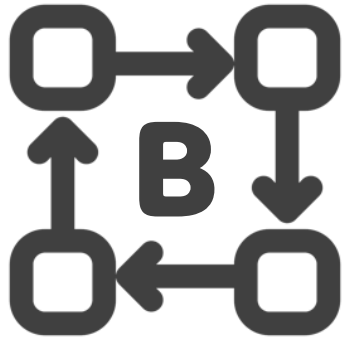
iD·One이 뭐 길래?

첫번째: 외부 해킹에 대한 걱정이 없는 블록체인 시스템

1

일반적인 구성은 1개 서버,
슈퍼 관리자 계정이 존재함,
기록에 대한 수정/삭제 가능,
외부 해킹에 취약함

VS



8000

퍼블릭 블록체인(이더리움) 구성은
약 8000개 노드, 슈퍼 관리자 계정이 없음,
기록에 대한 수정/삭제 불가능,
외부 해킹에 강함

일반 서버 구성과는 달리 블록체인 구성은 슈퍼 관리자 계정이 없어 시스템 전체를 해킹하는 것이 불가능

02-3

iD·One이 뭐 길래?

두번째: 사용자의 실제 지문과 얼굴의 생체정보로 인증하는 방식

지문정보 얼굴정보 사용자 확인

실제 카메라 인식을 통해 **본인의 지문과 얼굴 인식정보를 1:1 매칭하는 방식**으로 온/오프라인에서 등록된 완벽한 사용자 확인이 가능

02-4

iD·One이 뭐 길래?

세번째: 오픈API를 활용한 무한한 확장성

오픈API　　맞춤개발　　기능추가

인증이 필요한 모든 개발 플랫폼에 오픈API를 통해 안전하고 편리한 사용자 로그인 인증기능의 추가가 쉬움

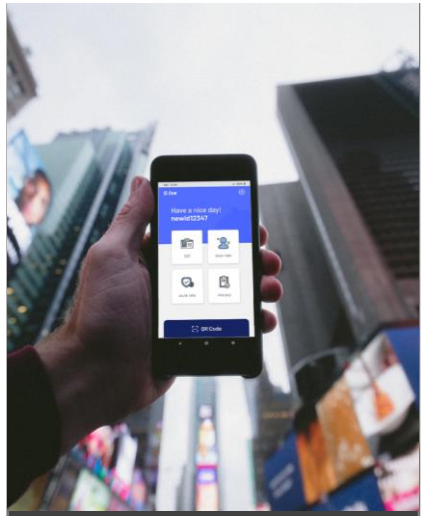
02-5

iD·One이 뭐 길래?

블록체인의 안전함과 완벽한 본인확인에 오픈API의 편리함을 더하다.

안전한
블록체인

완벽한
본인확인



편리한
오픈API

사용자의 단일 ID를 바탕으로 다양한 외부 계정 서비스를 하나로 연결하는 안전하고
완벽하며 편리한 자가인증 솔루션 iD·One 솔루션을 여러분께 추천합니다.

03

어떻게 이용하지?

iD·One 사용법 이렇게…

DIGENT iD

03-1

어떻게 이용하지?

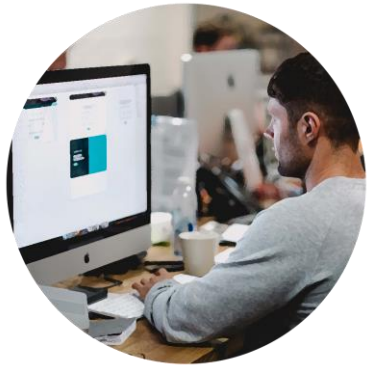
개인의 비밀번호 없는 접속권한

로그인 및 회원가입

사용자는 통합 iD로
iD·One 솔루션이 적용된
모든 플랫폼에 회원가입
절차없이 로그인 및
이용이 가능하다.

개인 정보관리

사용자의 개인정보를
인증기업(이통사, 금융사 등)
제3자가 관리하지 않고
사용자가 관리한다.
(개인정보의 탈중앙화)



갱신 없는 사용자 증명

사용자는 한번 가입으로
자신의 ID 및 자가 인증
서비스를 평생 갱신 없이
사용 할 수 있다.
(평생 무료/부분 유료)

개인의 온/오프라인 서비스에서 iD·One 하나면 충분합니다.

03-2

어떻게 이용하지?

기업의 응용 비즈니스

기업 통합인증(SSO)

기업은 통합 iD로 회사의
모든 온/오프라인 접속관리가
가능하고 기존 사원증을
대체 할 수 있다.
(Single Sign On)

기업 보안영역

기업은 회사의 민감한 보안이
필요한 영역에서 사원이 회사의
자료나 출입에 필요한 접근 시
자격증명과 출입관리가
가능하다.

온/오프라인 서비스

기업은 회사가 서비스하는
온/오프라인 플랫폼 서비스에
사용자 회원정보 관리 및 인증
수단으로 사용한다.
(웹 서비스 로그인)

기업의 내부/외부 서비스 통합도 iD·One 하나면 충분합니다.

03-3

어떻게 이용하지?

금융서비스의 자격증명

공인인증서 대체수단

기존의 공인 인증서의
인증 수단을 대체
할 수 있다.
(공인인증서 제도 폐지)

금융정보 이용수단

금융의 예금, 출금, 이체, 조회,
대출, 보험 등의 금융상품을
이용시 인증수단으로
사용한다.

신용카드 보안수단

신용카드의 금융사고를
방지하고 결제 인증수단으로
사용한다.
(각종 디지털 화폐 포함)

금융 서비스의 차세대 통합도 iD·One 하나면 충분합니다.

03-4

어떻게 이용하지?

정부/공공기관의 인증 통합

신분증의 보조수단

기존의 주민등록증, 운전면허증,
외국인등록증, 여권 등 신분증을
보조수단으로 사용한다.
(디지털 ID 서비스)

디지털 신분증(DID)

기존의 신분증을 별도의 서비스
플랫폼 개발이나 추가 작업 없이
디지털 신분증으로 변환이
가능하다.
(DID 전용 솔루션 불필요)

인증 통합 관리수단

자가인증과 디지털 신분증으로
각종 신분증을 통합하여 안정적이고
편리한 사용자 관리수단이
가능하다.
(공무원증, 인허가증 등)

정부/공공기관 인증 통합도 iD·One 하나면 충분합니다.

03-5

어떻게 이용하지?

iD·One 적용 시나리오

개인의 비밀번호 없는 접속권한

- 로그인 및 회원가입
- 개인 정보관리
- 갱신 없는 사용자 증명

기업의 응용 비즈니스

- 기업 통합인증(SSO)
- 기업 사원증 대체수단
- 보안영역 자격증빙
- 보안영역 출입관리
- 온/오프라인 서비스
- 회원정보 관리수단
- 개인회원 인증수단

금융서비스의 자격증명

- 공인인증서 대체수단
- 금융정보 이용수단
- 예금/출금/이체/조회
- 대출/보험
- 신용카드 보안수단
- 각종 디지털 결제 인증수단

정부/공공기관의 인증 통합

- 신분증의 보조수단
- 주민등록증
- 운전면허증
- 외국인등록증
- 여권
- 디지털 신분증(DID)
- 인증 통합 관리수단

사용자는 iD·One으로 외부계정 로그인 서비스를 지원하는 모든 플랫폼 서비스에서 ID로 로그인과 본인인증 적용이 가능

03-6

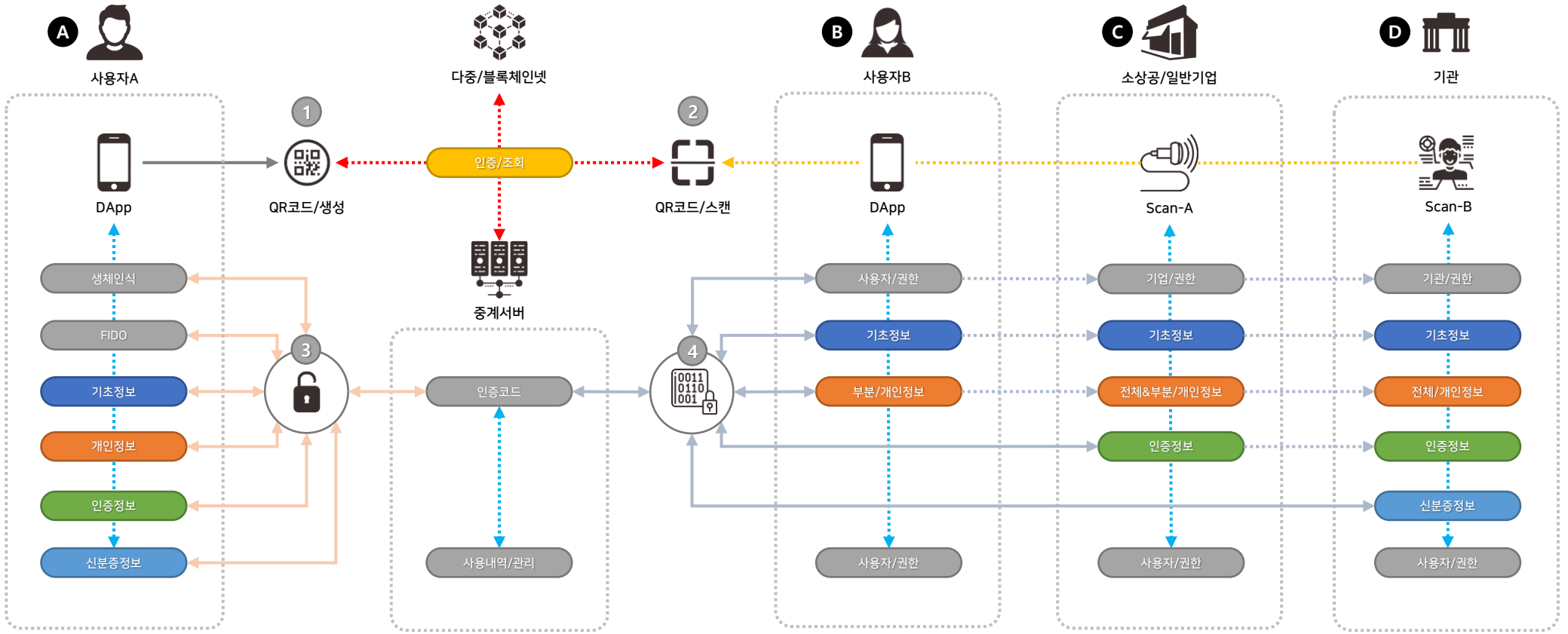
어떻게 이용하지?

로그인 본인 인증 솔루션 별 기능비교

기능	공인인증서	소셜(구글/네이버..)	iD·One
실제 본인 존재 증명	불가능(복사 가능)	불가능(다중 로그인 가능)	가능(복사 및 다중 로그인 불가)
실제 생체정보(지문/얼굴)	지원 안함(기능 없음)	지원 안함(기능 없음)	지원함(실제 생체정보)
PC 및 모바일 인증(A·OS/iOS)	지원함	지원함	지원함
FIDO 인증(지문/얼굴/패턴/PIN)	지원함	지원함	지원함
아이디	없음	있음	있음
비밀번호	있음(비밀번호/OTP 등)	있음(비밀번호)	없음
개인정보 관리서버/관리자 계정	있음	있음	없음
블록체인 검증	없음(지원 안함)	없음(지원 안함)	있음
범용 로그인 지원	없음(지원 안함)	지원함(제한적)	지원함(확장가능)
QR코드 지원	불가능(기능 없음)	가능(제한적)	가능(확장가능)
오픈API 지원	지원 안함(기능 없음)	지원함(제한적)	지원함(확장가능)
오프라인 연결 지원	지원 안함(기능 없음)	지원 안함(기능 없음)	지원함(확장가능)

03-7

어떻게 이용하지?
iD·One 전체 프로세스



A. **사용자A:** 개인 사용자
B. **사용자B:** 개인 사용자, 1대1 거래자
C. **소상공/일반기업:** 온/오프라인 형태의 소상공(매장, 가게 등), 일반기업(스타트업, 중소기업, 대기업 등)
D. **기관:** 온/오프라인 형태의 정부, 공공기관, 금융기관 등

1. 사용자 본인/증명을 위해 모바일에서 인스턴트 QR코드를 생성한다.
2. 신분/증명 확인을 원하는 조회자(개인과 단체)는 사용자A의 QR코드를 스캔한다.
3. 사용자는 조회자가 QR코드를 스캔하여 본인의 정보에 접근할 수 있도록 조회자의 레벨에 따라 권한(인증)를 제공한다.
4. 조회자는 사용자가 제공한 인증코드를 통해서 조회자의 권한(인증)에 따라 사용자의 정보를 조회한다.

04

결과적으로 얻는 건?

기대효과 5가지

DIGENT iD

04-1

결과적으로 얻는 건?

첫번째 기대효과: ID가 하나다.

ID뭐지?

아~ 기억이…

VS

1

하나만 기억해…

사용자는 사용하는 플랫폼 서비스에 따라 다양한 ID를 만들 필요가 없다.

04-2

결과적으로 얻는 건?

두번째 기대효과: Password가 없다.

VS

✱✱✱✱✱✱

아~ 복잡해…

없음

없어…

사용자는 복잡한 규정의 Password를 기억 할 필요가 없다.

04-3

결과적으로 얻는 건?

세번째 기대효과: 개인정보를 저장하는 서버가 없다.

서버 있다

모두 거기 있네…

VS

서버 없다

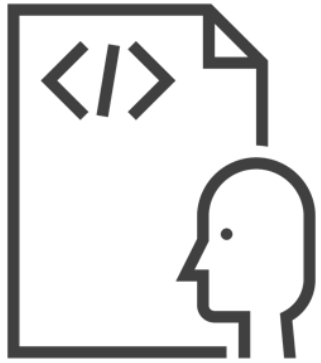
아~블록체인…

블록체인은 개인정보를 저장하는 물리적으로 연결된 서버가 없어 안전하다.

04-4

결과적으로 얻는 건?

네번째 기대효과: 오픈API로 누구나 쉽게 연결 할 수 있다.



개발 한다

개발 언어는…

VS

연결 한다

오~오픈API…

다양한 서비스 플랫폼의 로그인을 개발하지 않고 오픈API를 통해 쉽게 연결한다.

04-5

결과적으로 얻는 건?

다섯번째 기대효과: 기존 인증 솔루션에 비해 개발, 유지보수, 보안 비용이 싸다.

많이 든다

개발, 보안, 유비보수…

VS

적게 든다

개발, 보안, 유비보수…

기존 인증 솔루션에 비해 개발, 유지보수, 보안에 필요한 비용이 적게 든다.

05

어떻게 할거야?

향후계획

DIGENT·iD

05-1

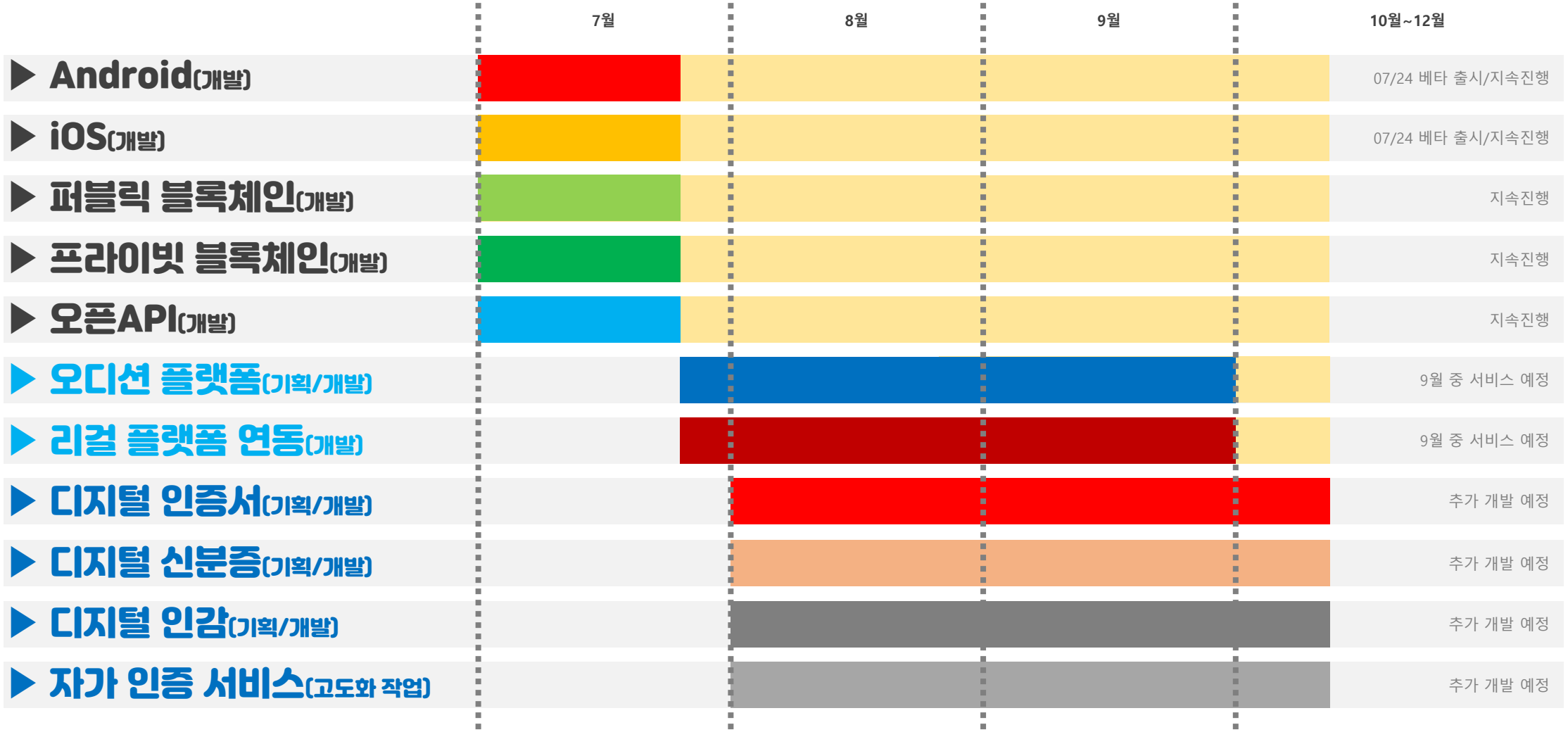
어떻게 할거야?

2020년 iD·One 솔루션 개발수준

05-2

어떻게 할거야?

2020년 iD·One 솔루션 개발일정



05-3

어떻게 할거야?

2020년 iD·One 마케팅 진행사항

◆ 글로벌 미디어 퍼블리싱 “파자마클라쓰” 오디션 플랫폼 - 공동 기획/개발 진행중

◆ 고려대 법창의센터 입주 협업 “쏠로” 법률상담 어플리케이션 - 로그인/인증 진행중

◆ 평택시 COVID-19 “QR·Pass” 다중시설 출입관리 어플리케이션 - 협의중

◆ 해양수산부 디지털 어업허가증 관리 어플리케이션 - 협의중

◆ 기업용 프라이빗 블록체인 기반 SSO(로그인/인증) 플랫폼 – 협의중

별첨

1. 그게 뭐지?

알려드려요

2. 질문 있어?

물어보세요

3. 넌 누구니?

회사소개

01

이게 뭐지?

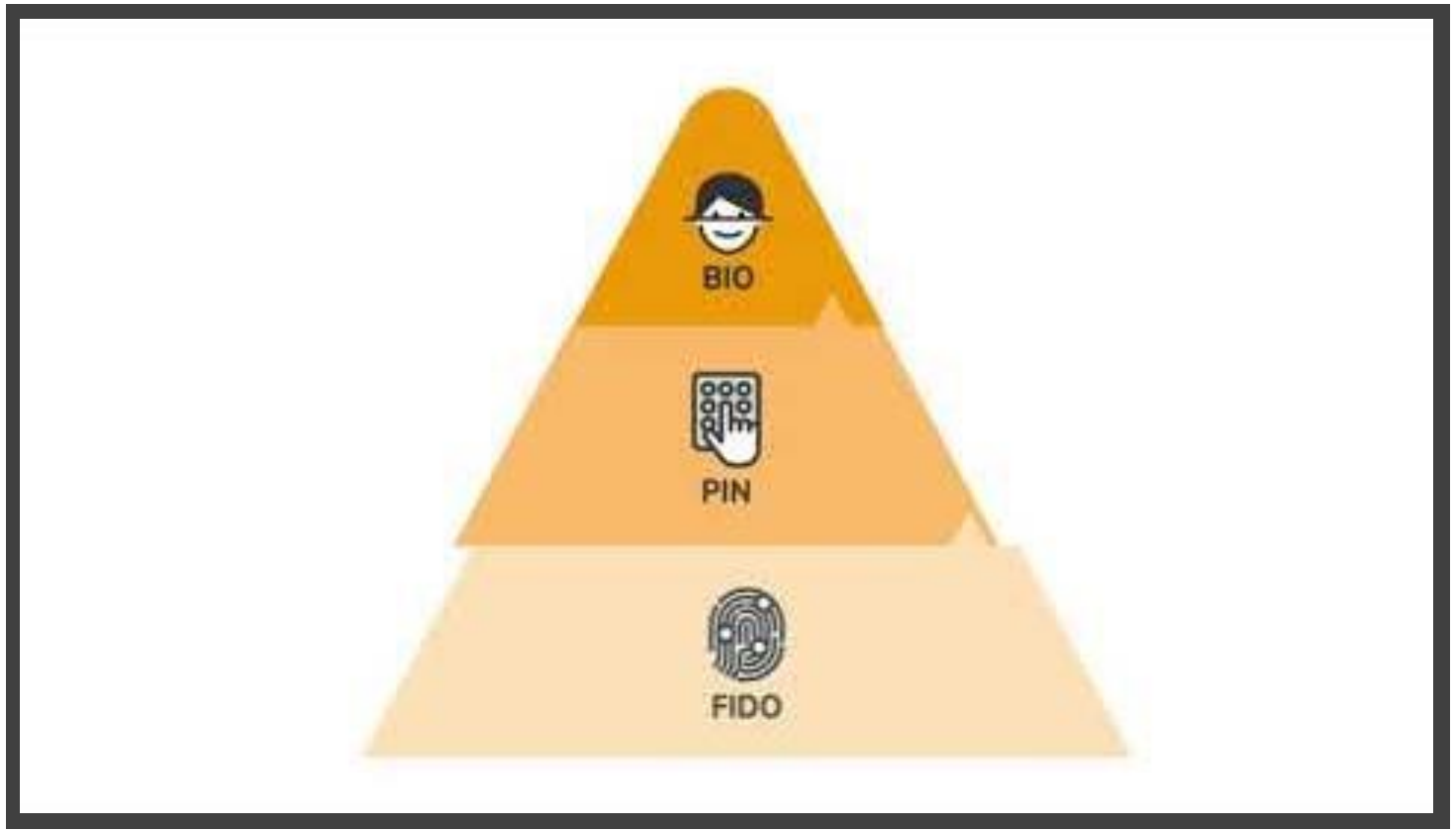
알려드려요

DIGENT iD

이게 뭐야?

iD·One 솔루션 소개

iD·One 소개영상



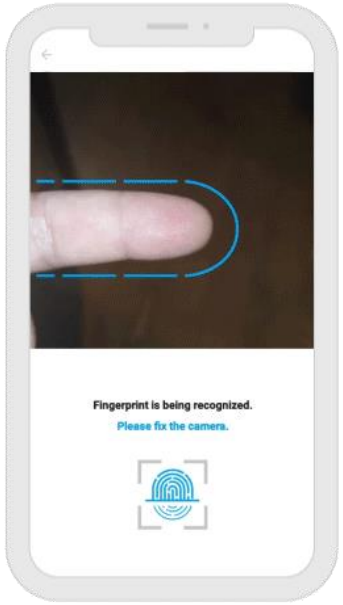
- 영상링크: https://www.youtube.com/watch?v=xglVRD-IE1s

01-2

이게 뭐야?

iD·One에 적용한 검증된 알고리즘

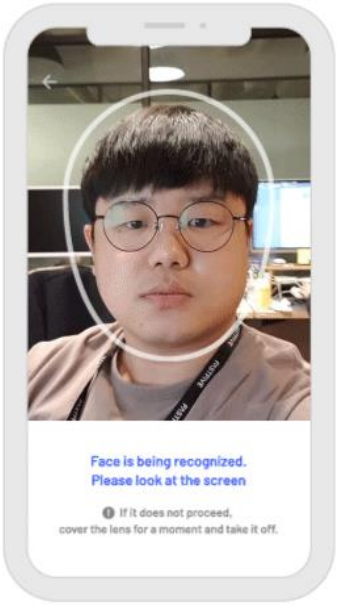
DIGENT



TECHNOLOGY

지문인식 알고리즘

Alchera



TECHNOLOGY

얼굴인식 알고리즘

selvas

TECHNOLOGY

국내 OCR 알고리즘

01-3

이게 뭐야?

iD·One에 적용된 멀티 블록체인

BLOCKCHAIN

퍼블릭 블록체인

ethereum

EOS

TRON

BLOCKCHAIN

프라이빗 블록체인

ethereum

HYPERLEDGER

02

질문 있어?

물어보세요

DIGENT·iD

02-1

질문 있어?

iD·One 관련 Q&A

Q 리얼 생체정보를 활용한다는 게 뭐가 다르다는 건가?

A 생체정보를 표방하는 인증방식 대부분이 FIDO프로토콜을 활용한 지문 센서나 안면인식을 활용한다.

iD·One도 FIDO 프로토콜을 사용하지만 민감하고 중요한 사안에는 BIO인증을 사용한다.

FIDO는 간편하긴 하지만 단말기에 복수의 생체정보를 등록할 수 있기 때문에 타인 도용의 가능성을 완전 배제할 수 없다.

iD·One은 본인의 리얼 생체정보만을 인증에 활용하므로 타인도용의 가능성으로부터 자유롭다.

Q 블록체인 기술을 구체적으로 어떻게 활용하는가?

A 회원의 개인정보를 저장하는 방식에 블록체인을 활용한다.

기존 블록체인 인증이 대부분 하이퍼레저를 쓰지만 iD·One은 퍼블릭 블록체인 기반으로 시스템을 구현한다.

현재 이더리움, 이오스, 트론, 프라이빗 이더리움으로 구성되어 있으며 네트워크 상태에 따라 스위칭 된다.

기존 하이퍼레저 기반의 블록체인과 비교했을 때 저렴한 유지비용, 현존하는 가장 강력한 데이터 보안, 글로벌 확장성 등의 이점을 누릴 수 있다.

02-2

질문 있어?

iD·One 관련 Q&A

Q 자가인증(Self Authentication)의 개념이 뭔가.

A 나의 개인정보와 인증키를 보관하는 외부의 사업자(네이버,구글,이동통신사 Etc...)에 의해 신원을 증명하는 것이 아니라 사용자 본인이 블록체인에 올린 개인정보를 활용하는 방식이기 때문에 제 3자 인증(3rd Party Authentication)과 구분되는 개념으로 쓴다.

이 과정에서 iD·One은 API의 중계만을 담당할 뿐 사용자정보에 대한 접근,저장,소유,편집에 대한 어떠한 권한도 갖고 있지 않다.

바로 이점이 개인정보 데이터서버를 운영해야 하는 기존 인증방식과 다른 점이다.

Q 휴대폰이 바뀌거나 초기화될 경우 어떻게 되나.

A iD·One은 구조상 휴대폰이나 서버에 회원의 개인정보가 저장되지 않아 물리적으로 해킹이 어렵다.

현재 기존의 휴대폰 단말기의 특정 영역에 저장하는 방식이 각광 받고 있지만, iD·One의 개인정보를 저장하지 않는 방식이 더 안전하다.

휴대폰이 바뀌거나 초기화될 경우에도 iD·One은 블록체인에 등록한 자신의 생체정보를 기준으로 본인의 계정을 복구할 수 있다.

03

넌 누구니?

회사소개

DIGENT iD

03

넌 누구니?

회사소개

❖ DIGENT (Digent Co., Ltd)

- 주식회사 디젠트는 2000년 설립된 지문 및 생체인증 토탈 솔루션 제공업체로서 행정자치부, 법무부, 경찰청, 인천공항 등 다수의 정부와 공공기관에 자체 알고리즘 및 제품을 제공하고 있습니다.
- www.digent.com

❖ DIGENT·iD (Digent ID Co., Ltd.)

- 주식회사 디젠트아이디는 주식회사 디젠트의 자회사로서 디젠트의 검증된 생체인증 기술에 빅데이터, 블록체인 등 4차 산업 기술을 접목하여 더욱 발전된 멀티 인증 솔루션을 개발하기 위하여 2018년 설립된 회사입니다.
- www.digentid.com / www.idone.io

응용

1. iD·One의 제안

방역 출입관리

2. iD·One의 제안

보훈 헬스케어

iD·One의 제안

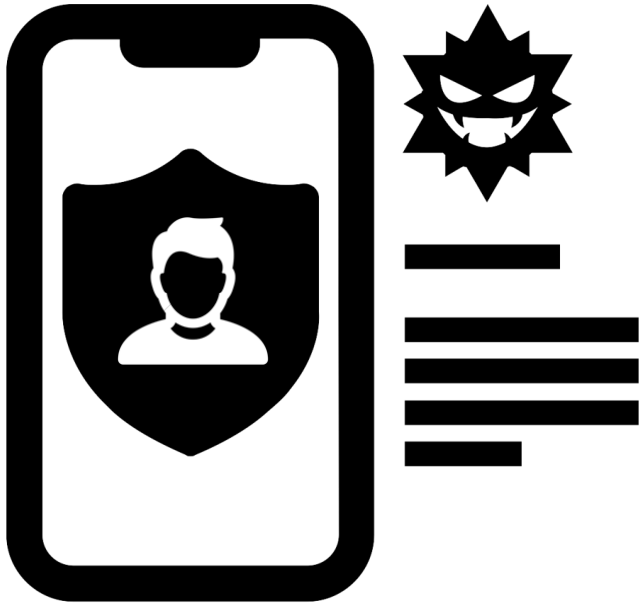
방역 출입관리

한국형 COVID-19 출입관리 서비스

01-1

iD·One의 제안

안정적인 출입자 추적 시스템의 필요성



이태원클럽 집단감염 발생으로 인하여 클럽, 유흥음식점, 주점, PC 방, 노래방 등 다중 출입시설에 대한 정확한 출입자 기록을 확보할 수 있는 방안이 절대적으로 필요해 짐.

- ❖ 정부/광역지자체 입장에서 행정명령(집합금지명령)을 통한 해당 출입시설의 운영금지를 장기간 유지하기 어려움
- ❖ 클럽, 유흥음식점, 주점 등을 이용한 방문자 중 전화번호 허위기재 다수
- ❖ 감염자가 발생시 이들을 추적하기 위해 막대한 행정력(인력, 시간, 비용) 소모
  - CCTV분석, 통신사 기지국 접속기록 확보, 신용카드 결제 내역 조회 등
- ❖ 또한 이 과정에서 개인정보 보호의 중요성이 커짐

01-2

iD·One의 제안

QR·Pass 솔루션 전체 프로세스

A. 이용자 등록 프로세스

- 이용자
- 앱 다운로드
- 이용자ID 생성, 휴대전화 본인인증, PIN 입력
- 앱 가입 완료

B. 출입시설 등록 프로세스

- 출입시설
- 출입시설 정보 등록
- QR코드 스티커 발급
- 출입시설 QR코드 스티커 부착

C. 출입시설 입장 프로세스

- 이용자
- 출입시설 방문
- QR코드 스티커 스캔
- 출입정보 관리 시스템 이용자 출입정보 조회
- 이용자 앱 알림 메시지 확인
- 출입시설 관리자 앱 메시지 확인후 입장진행

01-3

iD·One의 제안

QR·Pass 솔루션(준비단계)

이용자

앱 다운로드 및 등록

- Android 플레이 또는 iOS 앱스토어에서 앱 다운로드
- 국내 통신사(KT, SKT, LGU+, 알뜰폰 등) 휴대전화 본인인증으로 전화번호 확인
- 생체 정보 등록(선택 사항) 및 PIN 생성
- 블록 체인에 개인 정보 등록
- 등록 완료

솔루션 개발사

API 연결

- **API연결을 통해 정부/광역지자체의** 기관에서 관리

Blockchain

- 자신이 개인정보 관리주체
- 블록체인에 개인정보 등록/조회

출입시설

출입시설 QR코드

- 출입시설에 QR 코드를 **정부/광역지자체의** 기관에서 발급
- 출입시설 입구에 QR 코드 스티커 부착

정부/광역지자체

이용자 모니터링 시스템

- 출입시설 이용자 실시간 모니터링

출입시설 QR코드 발급 시스템

- 출입시설 QR코드 발급

출입시설 이용자 DB 서버

- 출입시설 및 이용자 실시간 이용정보 저장

01-4

iD·One의 제안

QR·Pass 솔루션(이용단계)

이용자(1인)

QR코드 이용자 리더앱 실행
- 입장하기전 출입구에 부착된 QR코드 스티커를 모바일 앱으로 스캔
- 출입시설/관리자에게 앱 메시지 재시 후 입장

출입시설/관리자

출입시설 QR코드 스캔
- 관리자는 QR코드가 체크된 이용자의 앱 메시지를 확인 후 입장진행

온라인/네트워크

블록체인 네트워크
- 블록체인 네트워크에 암호화된 이용자 개인정보를 복호화하여 사용자 정보를 조회

API연결
- 이용자의 출입시설 이용정보(이용자 ID, 연락처, 출입시설 정보, 이용시간)를 정부/광역지자체의 출입시설 이용자 관리 시스템 및 데이터 처리 서버에 제공

정부/광역지자체

출입시설 이용자 관리 시스템
- 출입시설 이용자에 대한 실시간 이용정보 확인 및 모니터링이 가능

출입시설 이용자 DB 서버
- 출입시설 이용자 입장정보 처리 및 관리
- 이용자의 출입시설 출입정보는 일정기간 보관 후(약 15일~30일) 삭제

01-5

iD·One의 제안

QR·Pass 솔루션(비상상황)

정부/광역지자체

출입시설 이용자 관리

- **출입시설 이용자 감염상황 즉각 대응**
- **감염우려 이용시설 적정인원 초과여부 확인**
- **출입시설 감염우려 통보**
- **감염발생(코로나19 등)에 대한 즉각 초치**
- **감염상황 발생 출입시설 및 이용자에 대한** 감염(우려/발생)상황 및 대응 메시지 알림

이용자(1인)

QR코드 이용자 리더앱 알림

- 이용자가 출입한 출입시설에 대한 감염(우려/발생)상황 및 대응 메시지 알림
- 감염(우려/발생)상황 및 대응에 따른 행동지침 알림 및 감염 검사소 안내

출입시설

출입시설 관리

- 출입시설에 대한 감염(우려/발생)상황 및 대응 메시지 알림
- 출입시설 관리자가 정부/광역지자체의 감염상황 통보에 따라 즉각 **조치(출입시설 폐쇄 및 방역실시)**

01-6

iD·One의 제안

QR·Pass 솔루션의 장점

이용자

- QR코드/스캔으로 입장절차 간소화
- 신분증 제시 및 이름, 휴대전화번호의 현장기록 필요 없음
- 출입시설에 대한 개인정보 노출우려 낮음
- 블록체인 보안으로 개인정보의 해킹위험이 낮음
- 정부/광역지자체에 최소한의 개인정보 및 이용정보(이용자ID, 연락처, 출입시설 정보, 이용시간) 제공

출입시설

- QR코드 스티커로 입장절차 간소화
- 관리자의 이용자 신분증 확인 및 이름, 휴대전화번호 기록이 필요 없음

정부/광역지자체

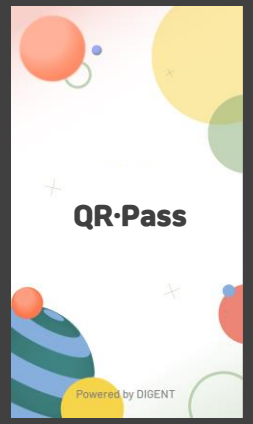
- 다중 출입시설에 대한 실시간 모니터링을 통해 감염자 발생시에 즉각 대응
- 이용자 밀집도 분석을 통해 감염우려 상황에 즉각 대응
- 출입시설 이용자에 대한 검증된 데이터 확보
- 비상상황(감염발생) 발생시 외부 협조(경찰, 통신사, 카드사 등) 이전에 자체 방역추적 대응
- 개인정보수집의 최소화

01-7

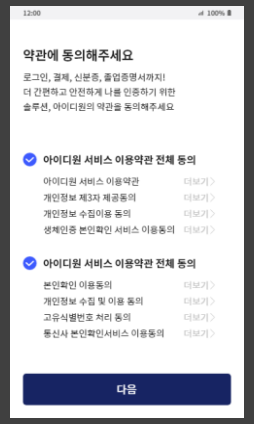
iD·One의 제안

QR·Pass 앱 UI 디자인(한국어 버전)

인트로

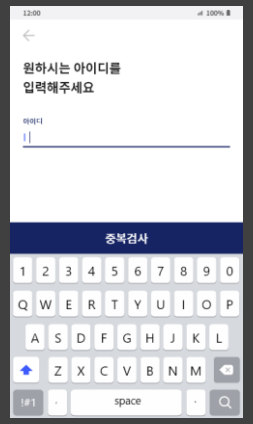


약관동의

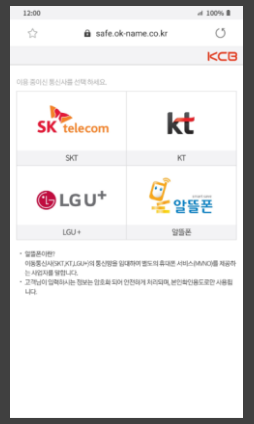


회원가입

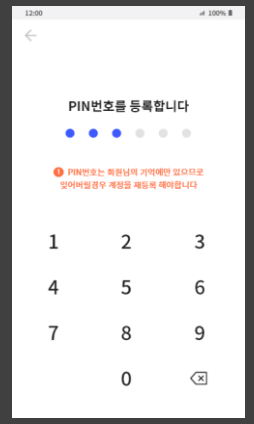
ID 생성



휴대전화 본인인증



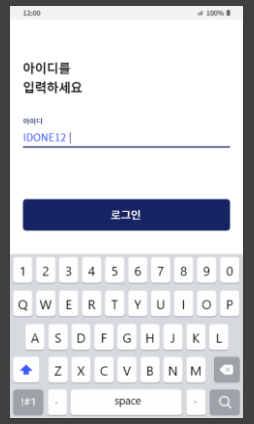
PIN 생성



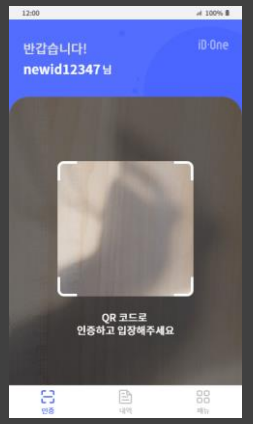
블록체인 등록

가입완료

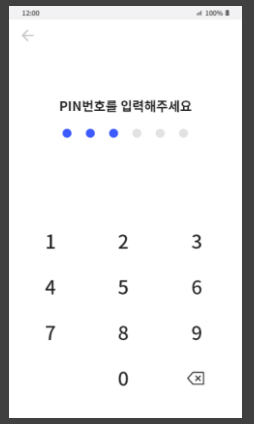
로그인



QR코드 스캔

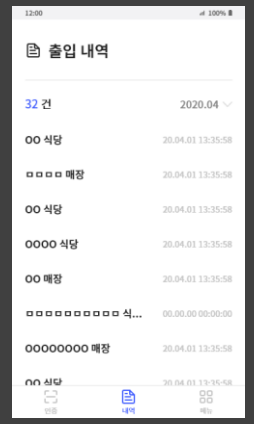


PIN 입력



요청 확인

이용 내역



01-8

iD·One의 제안

QR·Pass 관련 Q&A

Q 개인정보 유출방지를 위한 조치

A 모든 솔루션은 DB서버에 개인정보를 포함한 회원정보를 저장하고 여기서부터 사용자의 개인정보 유출문제가 시작된다.

기존 출입관리 솔루션은 이름, 성별, 생년월일, 휴대전화번호의 4가지 정보에 출입시설 위치정보 및 이용시간을 기록하고 개인정보를 일정기간 보관하다 기간이 지나면 서버 기록을 삭제하지만 서버가 해킹이 되는 경우 개인을 특정 할 수 있는 개인정보가 유출된다.

"QR·Pass" 출입관리 솔루션은 휴대전화 본인인증을 거친 휴대전화번호만을 암호화 시켜 기록하고 암호화된 휴대전화번호 정보가 해킹되어도 이름, 성별, 생년월일 등의 매칭 정보가 없어 개인을 특정할 수가 없다.

Q 다른 출입관리 솔루션 대비 장점

A 기존 출입관리 솔루션 이용자 개인정보는 전용 DB서버에 저장하는 방식으로 솔루션 구축 및 유지관리 비용이 높다.

"QR·Pass" 출입관리 솔루션은 사용자 본인이 블록체인 네트워크에 자신의 개인정보를 올리고 필요할 때 제공되는 방식이라 개인정보를 관리하는 별도의 DB서버가 존재하지 않는다.

"QR·Pass" 출입관리 솔루션 이용자 개인정보는 암호화된 블록체인 네트워크에 저장하는 방식으로 솔루션 구축 및 유지관리 비용이 낮다.

또한 휴대전화 본인인증을 거친 이용자의 정보만 수집되기 때문에 데이터의 신뢰성이 높다.

01-9

iD·One의 제안

QR·Pass 관련 Q&A

Q 집합공간의 사업주(관리자)가 해야 할 일은 ?

A 출입시설에는 정부/광역지자체에서 발급받은 사업장 고유 QR코드 스티커를 입구에 부착한 후 이용자가 QR코드 스티커를 스캔 후 확인된 앱 메시지를 관리자에게 보여주고 출입시설 입장을 진행한다.

정부/광역지자체의 행정기관이나 방역당국이 지정한 필수 사업장(클럽, 유흥음식점, 주점 등)은 발급된 지정 QR코드 스티커를 부착한다.

필수 사업장이 아닌 곳(교회, 기업, 놀이공원, 전시장, 택시 등)에서 고유번호를 부여 받고 싶다면, 지정 웹사이트 방문 후 간단한 사업주(관리자) 정보를 입력하고 고유 QR코드를 발급 받아 프린트하여 별도로 출입시설에 부착 할 수 있다.

Q 집합공간의 방문자가 해야 할 일은?

A "QR·Pass" 출입관리 앱(안드로이드, iOS)을 다운받아 설치하며 가입을 완료한다.

1회의 휴대전화 본인인증을 통해 가입 후 방문하는 모든 시설 입구에 부착된 지정 QR코드 스티커를 스캔하는 것 만으로 출입시설의 관리자에게 본인의 신분증이나 휴대전화번호를 제공할 필요가 없다.

출입시설에 이용자의 이름, 성별, 생년월일, 휴대전화번호 등의 개인정보가 일체 기록되지 않는다.

감염상황(우려/발생) 등 유사시를 위해 암호화된 이용자의 휴대전화번호만 정부/광역지자체의 행정기관이나 방역당국이 제공된다.

iD·One의 제안

보훈 헬스케어

한국형 블루버튼 헬스케어 솔루션

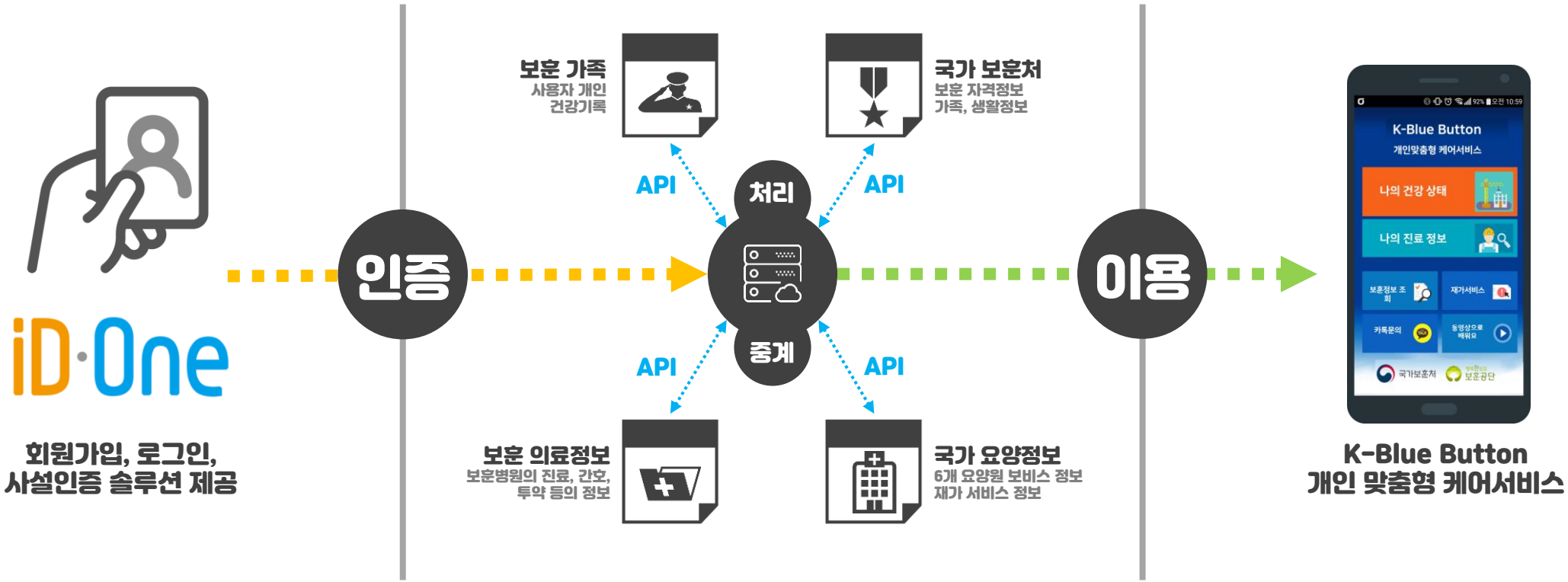
한국형 블루버튼(Blue Button) 서비스 구축의 필요성

- 보건의료체계 변화와 헬스케어 데이터는 다양한 형태로 의료기관, 정부 행정기관, 연구기관 및 개인 등에 분산되어 있기 때문에 **헬스케어 데이터 통합적 활용**이 중요한 과제
- 미국의 블루버튼 이니셔티브, 일본의 헬스케어 데이터 구축 정책 등 **선진국 주요 보건의료 정책**으로 진행 중
- 전국민 단위의 헬스케어 서비스를 실시하기전 테스트베드 역할로써 **200만 보훈가족을 대상으로 한 보훈헬스케어 서비스**를 추진
- 개인의 건강 및 생활환경 데이터 전반을 통합하여 **최적화된 의료 서비스 제공과 다양한 비즈니스, 공익사업 모델의 창출**이 가능

02-2

iD·One의 제안

서버간 오픈API 연결 프로세스



헬스케어 데이터 통합을 위한 마이그레이션은 많은 시간과 비용, 인력이 투입되며 서비스의 운영과 확장에 대한 경직성 문제가 발생

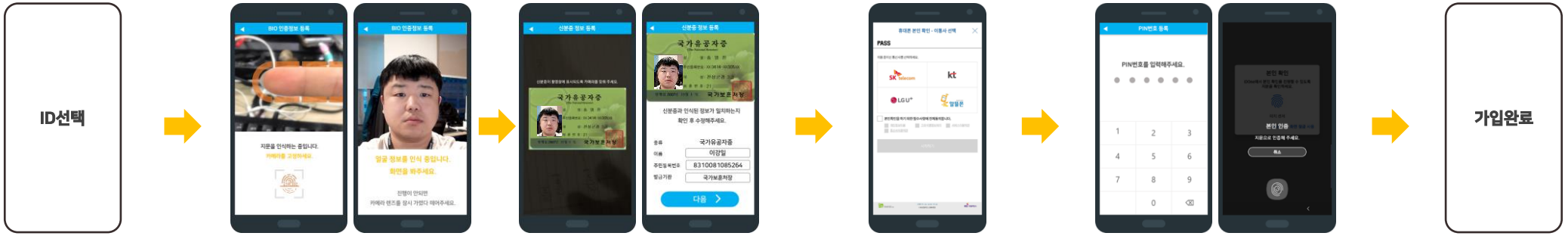
각기 다른 기관의 데이터를 통합하는 것이 아닌 API 방식의 서버간 통신으로 비용과 시간 리스크 최소화.

02-3

iD·One의 제안

iD·One 인증 솔루션 가입 프로세스

생성 → 실제 생체정보 인식 (지문/얼굴) → 보훈카드 등록 (OCR 인식) → 이통사 인증 (본인인증/SMS) → 모바일 기기 등록 (지문/PIN) → 완료



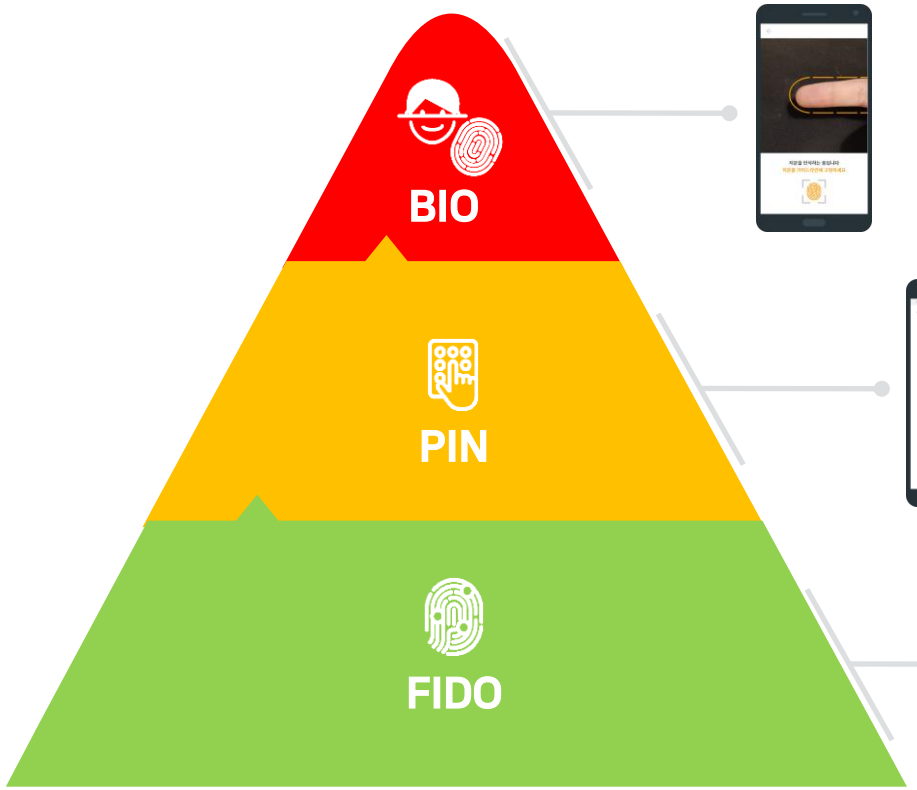
iD·One 자가인증 솔루션 특징

- ❖ 가입 후 비밀번호 없이 사용자는 모바일과 웹사이트에서 본인 인증이 가능
- ❖ 블록체인 방식의 자가 인증 솔루션으로 별도의 서버에 회원의 개인정보를 저장할 필요성이 없음
- ❖ 실제 생체정보 인증을 통해 민감한 의료기록의 열람, 저장, 전송 시 타인 인증 or 타인 도용의 가능성 원천적으로 차단

02-4

iD·One의 제안

iD·One 인증 솔루션의 접근 권한에 따른 인증 레벨



고수준 인증

사망기록, 처방기록, 진단기록, 장애기록 등의
민감한 정보의 열람, 전송 시

중수준 인증

보훈 서비스 신청, 개인정보의 열람,
전송,저장 등의 인증에 대응

저수준 인증

간편 회원가입, 로그인 등 비교적
낮은 수준의 인증에 대응

02-5

iD·One의 제안

iD·One 인증 솔루션의 도입효과

◆ 비밀번호없이 생체인증(지문 및 얼굴)을 통한 이용

→ 간단하고 사용하기 쉬움

◆ 개인정보는 이중 암호화되어 블록체인에 저장

→ 해킹의 위험 없음

◆ 고객의 정보를 저장하고 보호하기 위해 중앙 서버가 필요하지 않음

→ 기업의 해킹 방지 보안에 필요한 비용 절감

◆ 서비스 통합 인증 시스템을 통해 고객은 하나의 ID로 모든 온라인 서비스를 관리

→ 개인인증이 필요한 모든 부분을 하나로 통합 관리

◆ 온라인과 오프라인 모두 사용가능

→ 디지털 신원인증을 위한 우수한 플랫폼

감사합니다

DIGENT·iD

서울 강남구 강남대로 388 강남센타빌딩 16층 ㈜디젠트아이디
Tel : 02-3420-3140 / Fax : 02-3420-3009 / Web : www.idone.io / Email : info@idone.io