라온시큐업 2021

BEYOND THE DIGITAL WORLD

RAON

대한민국 최초의 디지털신분증

라온시큐어 김봉근 팀장

2021/11

INDEX

라온시큐업 2021

BEYOND THE DIGITAL WORLD

RAON

01 디지털 신분증

아낌없이 알려드리는 대한민국 최초의 디지털 신분증

디지털 신분증

대한민국 3대 신분증

	주민등록증	여권	운전면허증
			
주관기관	행정안전부	외교부	경찰청
근거법령	주민등록법	여권법	도로교통법
형태	플라스틱 카드 (위변조 방지기술 적용)	IC 칩이 탑재된 전자여권 **(유일)**	플라스틱 카드 (위변조 방지기술 적용)

정부기관이 근거 법령에 의해 발급함으로써

국가가 개인의 신분을 공식 증명하는 문서

그러나, 現 신원증명체계는...

본인확인 수단 "혼재"

오프라인

금융기관
공공기관

실물카드로
신원확인

위변조 및 도용 우려

- 개인정보가 공개된실물 플라스틱 카드로 신원 확인
- 상시 휴대 불편, 훼손 위험
- 위 변조 및 도용 우려 상존

온라인

휴대폰인증
소셜인증
공동인증서

서비스
제공기업

개인정보유출 취약

- 공동인증서, 휴대폰 인증 등 다양한 인증체계 활용
- 개별 서비스 제공기업에 개인정보 집중되어 대량 개인정보 유출에 취약

개인정보 유출에 취약한 구조

2022년 1월이 되면,
새로운 운전면허증 서비스가 찾아옵니다.

모바일 운전면허증 앱

전자여권과 동일한 IC칩이 탑재된 스마트 운전면허증

휴대폰 하나로 어디서든
내가 원하는 정보로 신원을 인증

발급/운영기관

발급 KoROAD 도로교통공단

운영 KOMSCO 한국조폐공사

공신력 있는
신분증 발급/운영기관

이용자

자기주권 신원 (SSI)
온-오프라인 통합인증

*SSI : Self-Sovereign Identity

서비스 제공기관

공공	공공웹 인증	증명서 발급	...
금융	은행 계좌개설	증명서 발급	...
민간	렌터카 이용	편의점 성인인증	...

신원검증

분산신원증명(DID) 블록체인 플랫폼

국가신분증으로서
공신력보장

안전하고 신뢰할 수 있는
국가 공통 플랫폼 구축

유용하고 쓰임새 많은
국민 체감형 서비스 확대

02 디지털 신분증의 목표

디지털 신분증의 목표

민간의 유사 서비스와는 근본적으로 다른 全 국민 대상 국가 신분증 구축

	국가 모바일 운전면허증	민간 본인확인 서비스
절차	IC 카드: 신청 → 본인 확인 → 칩 발급 → 발급 처리 → 교부 모바일 앱: 앱 실행 → 안면 인증 → ID 카드 태깅 인증 → 발급 등록 → 발급 완료 **엄격한 신분증 발급절차**	가입 → 본인 확인 → 면허증 촬영 → 휴대폰 인증 → 운전자격증명 저장 → 등록 완료 **기 등록된 신분증 단순 조회서비스**
기술	탈중앙화 신원 인증 (DID)	중앙집중형 신원 인증(CID)
증명주체	사용자 중심(자기 주권 신원 증명)	서비스 제공자 중심
용도	범용적 활용(신분증과 동일 효력)	제한적 활용(편의점 성인인증 등)

*DID : Decentralized Identifier CID : Centralized Identifier

특징

- 신분증의 공신력을 보장하는 발급절차 설계 중요
- 全 국민 대상의 국가적 디지털 전환사업
- DID 기술 기반 자기주권 신원증명 본격 적용

03 엄격한 신분증 발급 절차

엄격한 신분증 발급 절차

신분증 全 라이프사이클에 걸쳐 신뢰성 보장

국민의 우려

나 몰래 다른 사람이
내 신분증 발급받으면?

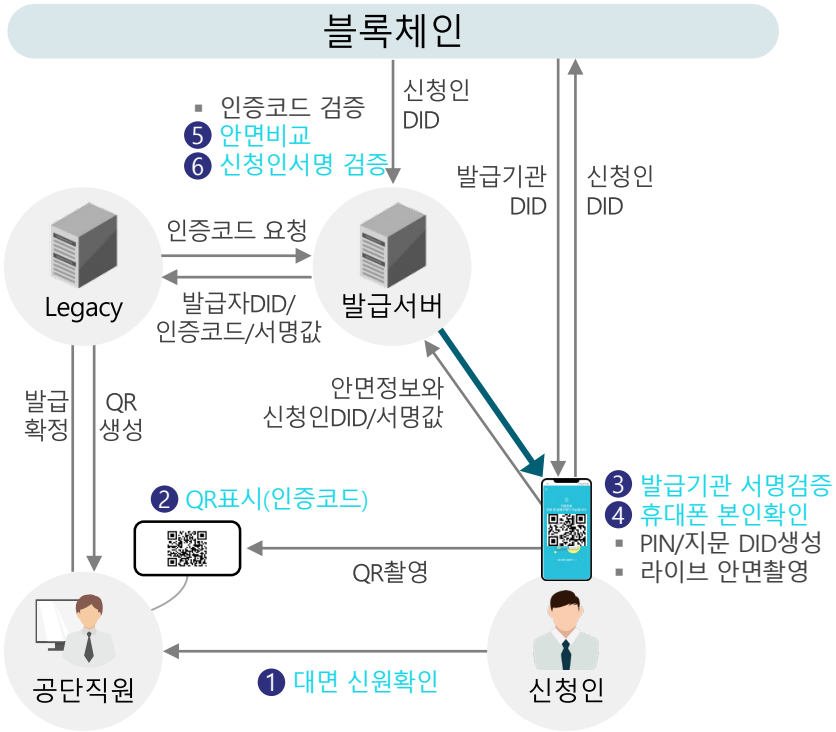
예상할 수 있는 시나리오

- 非신청자가 자신의 폰으로 발급 시도
- 신청자가 타인 폰으로 발급 시도
- 非신청자가 신청자 폰으로 발급 시도
- 피싱 사이트를 통한 발급 신청 유도

신분증 발급 3원칙

1. 반드시 정당한 신청자에게만 발급
2. 반드시 대면 확인한 신청자 본인의 휴대폰에만 발급
3. 발급시스템의 신뢰성을 증명

어떠한 불법적 시도도 허용하지 않는 철저한 신원검증 절차



신분증 발급 3원칙에 기반한
6단계 인증 적용

1. 최초발급 시 대면 신원확인
2. 신청인 전용 QR생성/검증
3. 발급기관 서명값 검증
4. 휴대폰 본인확인
5. 면허사진 vs 촬영 안면 비교
6. 신청인 서명값 검증

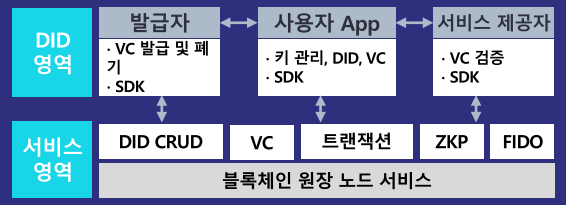
- 강력한 6단계 인증절차를 통해 신청인과 모바일 신분증 간 Strong Binding 보장
- 철저한 신원검증 절차 적용으로 국가 신분증으로 공신력 및 신뢰성 보장

국내 최다 적용사례에서 완성도가 입증된 DID 플랫폼 적용

국내 최다 DID 적용사례 보유

- 금융결제원 뱅크사인 DID 전환사업 ('21) — 국내 최고 보안수준
- 행안부 모바일 공무원증 ('20) — 본 사업 선행사업
- 병무청 본인확인용 블록체인 간편인증 ('19)
- 세종시 블록체인 기반 자율주행차 신뢰플랫폼 ('20)
- 경상남도 DID 기반 디지털 공공서비스 ('19) 외 다수 사례

"보안성이 뛰어난 DID플랫폼"



- 블록체인 기반 DID 플랫폼 최초 GS 인증 1등급 획득
- FIPS/KCMVP 암호인증 보유
- 외부 모듈 연동이 아닌 생체인증 모듈 탑재
- 보안전문 기술력 기반 개발

병무청 적용사례

- 공인인증서 대체한 공공기관 최초 블록체인 기반 DID 간편인증 및 부인방지 체계 구현
- 과기정통부 신기술 전자서명 우수사례 지정 (2019)

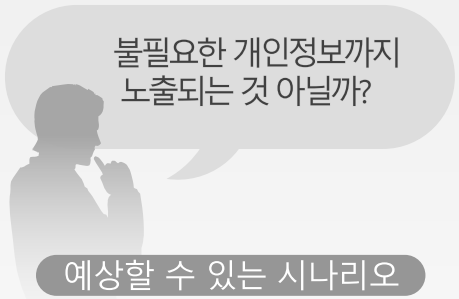
DID발급건수
28만 3천건

DID인증건수
225만 건

2021.5.17 기준

사용자 중심 자기주권 신원 증명

국민의 우려



예상할 수 있는 시나리오

- 단순 성인 확인이 필요한 상황에서 내 주민번호까지 보여줘야 하나,
- 신분증을 보여주더라도 내가 원하는 정보만 선별해서 보여줄 수 없을까.

상황에 맞게 꼭 필요한 정보만으로 신원 증명의 신뢰성 확보

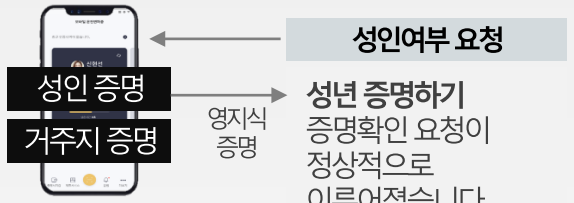
다양한 사용환경, 제출용도에 따른
온/오프라인 통합 신원 자격증명

오프라인 편의점에서 주류 구매
온라인 휴대폰 설문조사
온라인 홈택스 연말정산 로그인
오프라인 경찰관에게 면허증 제시
온라인 은행 대면/비대면 계좌개설

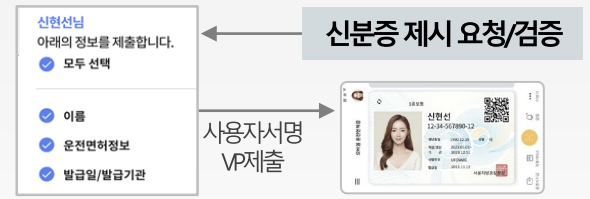
Bluetooth Low Energy / NFC / 인터넷

다양한 통신수단

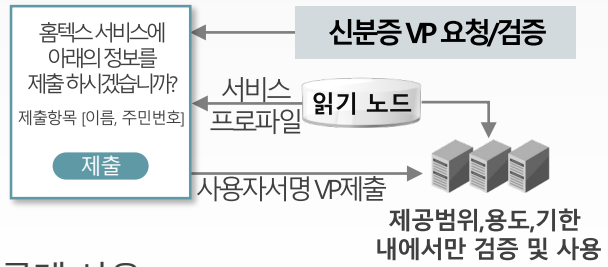
영지식 기반 개인정보 노출 無



DID 기반 선택적 제공으로 도용 방지



사전 허가된 정책기반 정보제공



- 영지식부터 실명증표까지 개인이 목적에 따라 자유롭게 사용
- 자기주권신원(SSI)에 따라 제출용도, 사용환경별 최소한의 범위로 정보를 제공

*영지식(ZKP) : Zero-Knowledge Proof, 상대방에게 어떠한 정보도 제공하지 않고, 자신이 해당정보를 소유하고 있다는 사실을 증명

신분증 사용 3원칙에 근거한 범용적 사용(신분증과 동일효력)

국민의 우려

내 신분을 확인하려는
상대방은 과연 믿을 수 있나?

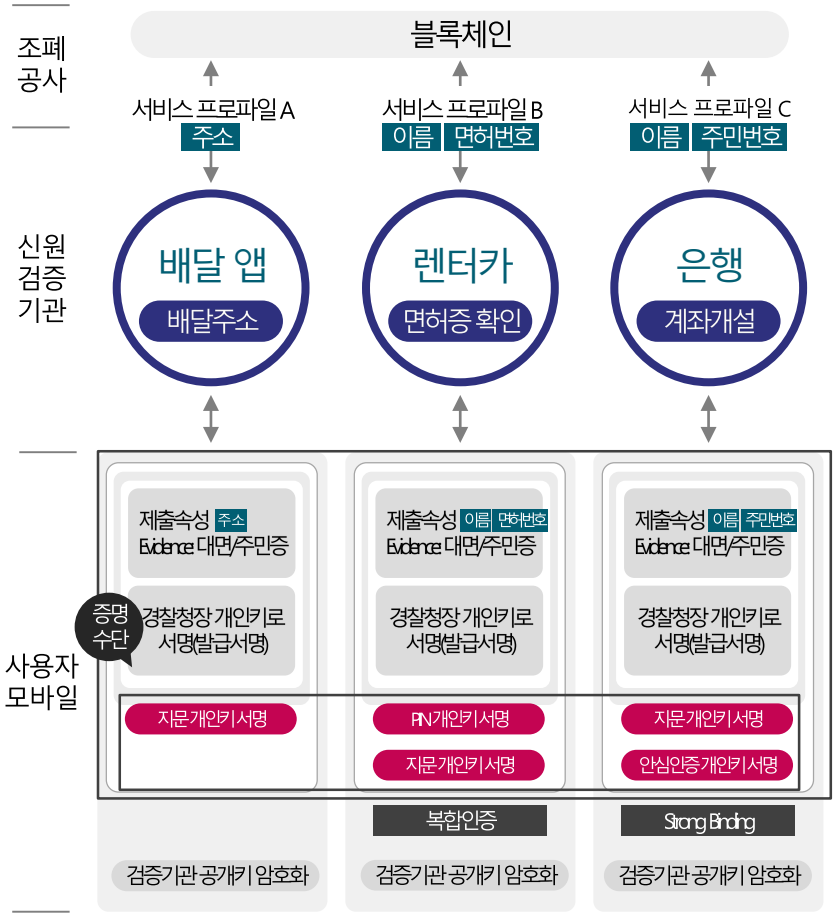
예상할 수 있는 시나리오

- 허가받지 않은 기관이 내 신원정보를 가져가려는 시도
- 신원확인자가 과도한 개인정보를 요구

신분증 사용 3 원칙

1. 사전에 허가된 검증기관임을 보장
2. 사전에 정의된 개인정보 범위 限에서만 정보 제공
3. 소유자와 사용자가 동일인을 보장

사전 신원검증기관 허가부터 사용까지 全 과정 보안성 확보



신원검증기관별 서비스 프로파일에 보안수준과 인증수단 사전허가

신원검증기관별 서비스보안 수준과 인증수단 사전허가

신분증 사용 시, 허가된 정보만 제출

사전에 정의된 최소한의 정보만 제출

사용자는 서비스별 증명수단으로 신분증 소유자와 동일인 증명

소유자와 실사용자가 동일인임을 증명수단으로 보장

04 디지털 신분증 발급

아낌없이 알려드리는 대한민국 최초의 디지털 신분증

디지털 신분증 발급

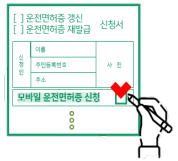
예시

1 면허시험장 방문

현 운전면허 발급장소인
전국 27개 시험장 직접 방문

2 발급신청서 작성

운전면허시험장에 비치된
신청서식 작성

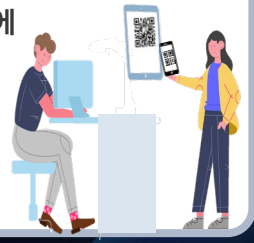


3 신원확인 및 접수

신분확인수단 : 신분증 /지문
본인 신원확인 후 창구담당자 접수
도로교통법 시행규칙 제82조의

4 1회용 발급 QR 제공

창구에 설치된 스크린에
발급용 QR 표출



5 모바일 운전면허증 발급

① 스마트폰 본인확인
② 1회용 발급 QR 촬영
③ 얼굴 및 면허사진 일치여부 확인

1 kt

2

3

4

6 인증 수단 등록

① 일반인증 등록
② 안심인증 등록

1

2 ****

일반인증시 사용할
인증수단 등록

안심인증시 사용할
인증수단 등록

발급완료

RAON

예시

현장 방문 발급 QR 생성 시 QR 내용은?

현장 발급QR 생성

- 신청인 대면 신원확인 완료 후 발급 확정과 동시에 발급 시스템에서 QR정보를 생성하고 전달

- 전달 된 QR정보는 현장 태블릿 장비에 QR로 표시

- 신청인은 모바일 신분증 App을 통해 발급QR을 스캔

■ 현장창구 직원을 통해서 생성되는 발급QR에는
발급기관DID, 넌스(NONCE)값, 타임스탬프, 신청자 인증코드, 발급기관서명정보가 포함되어 생성

발급 QR정보 상세 내용

종류	설명	비고
발급기관DID	발급QR을 생성하는 발급기관DID	발급기관DID에 해당하는 공개키를 블록체인을 통해 취득 후 서명검증 수행
NONCE	특정 발급 거래에 대한 식별자	NONCE 별 거래상태 관리 및 전체 발급거래를 식별
타임스탬프	QR 효력 시간제한 스탬프	QR에 대한 시간관리
신청자 인증코드	특정 신청인과 매핑정보 값	발급서버에서 신청인과 인증코드를 매핑관리 하여 신청자만 발급처리
발급기관 서명정보	발급기관 개인키로 발급QR정보를 서명한 값	발급기관 공개키를 통해 서명검증 수행 시 비교

검증 기관 QR정보 상세 내용

종류	설명	비고
검증기관DID	연계처리를 위해 QR을 생성하는 연계기관DID	사용자는 연계기관DID를 블록체인에서 확인하여, 연계기관의 정당성을 확인 해당 연계기관의 Profile을 획득하여, 연계기관에 제출해야 하는 속성정책 확인
NONCE	특정 검증 거래에 대한 식별자	검증 시, 발생하는 다수의 트랜잭션을 관리하기 위한 NONCE 값
타임스탬프	QR 효력 시간제한 스탬프	QR에 대한 시간관리
Call back url	신분증 VP의 제출목적지	검증을 수행하는 검증기관 url정보 (데이터 크기의 최소화를 위해, 연계기관 Profile 획득 시, 연계기관 DID 도큐먼트의 service-end-point내 설정 가능)

Q. 그렇다면, 휴대폰을 바꿀 때마다 면허시험장이나 경찰서에 가라는 말인가요?

안쓰고 말지

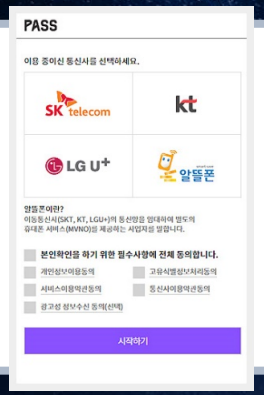
※'19년 기준 스마트폰 평균 교체 주기는 약 2년 9개월(조사기관 : 베이스트리트 리서치)

디지털 신분증 발급

예시

1 휴대폰 본인인증

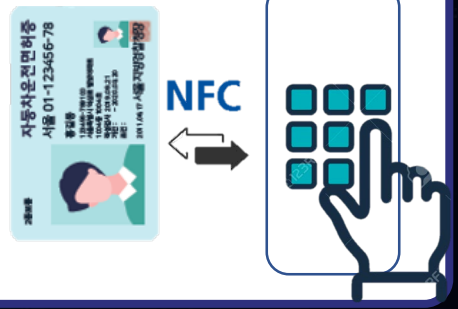
휴대폰 본인확인을 통해
스마트폰 점유확인 및
1인1단말 정책 담보



2 IC 카드 소유여부 확인

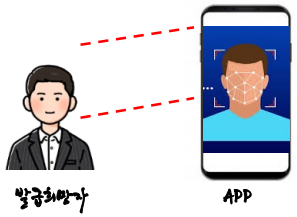
등록한 비밀번호를 입력하여
IC카드 확인

※ PIN 비밀번호를 암호화하여 IC카드에 전송 → 앱 발급 권한 획득

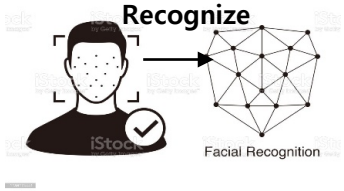


3 얼굴 및 면허사진 비교

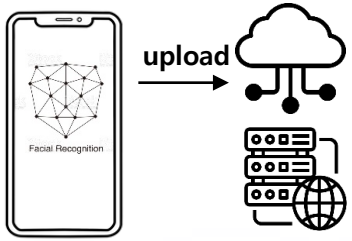
1 APP에서 발급희망자의 얼굴 촬영



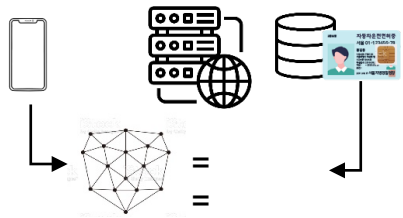
2 촬영한 사진에서 특징점 축출



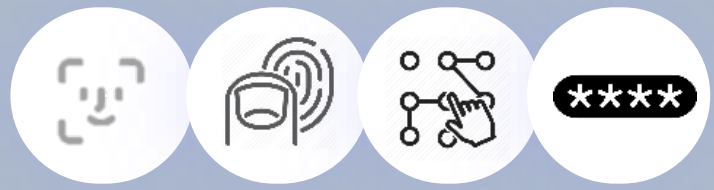
3 특징점 면허시스템에 전송



4 면허DB의 사진에서 특징점 축출 후 업로드 된 특징점과 일치 확인



4 인증수단 등록



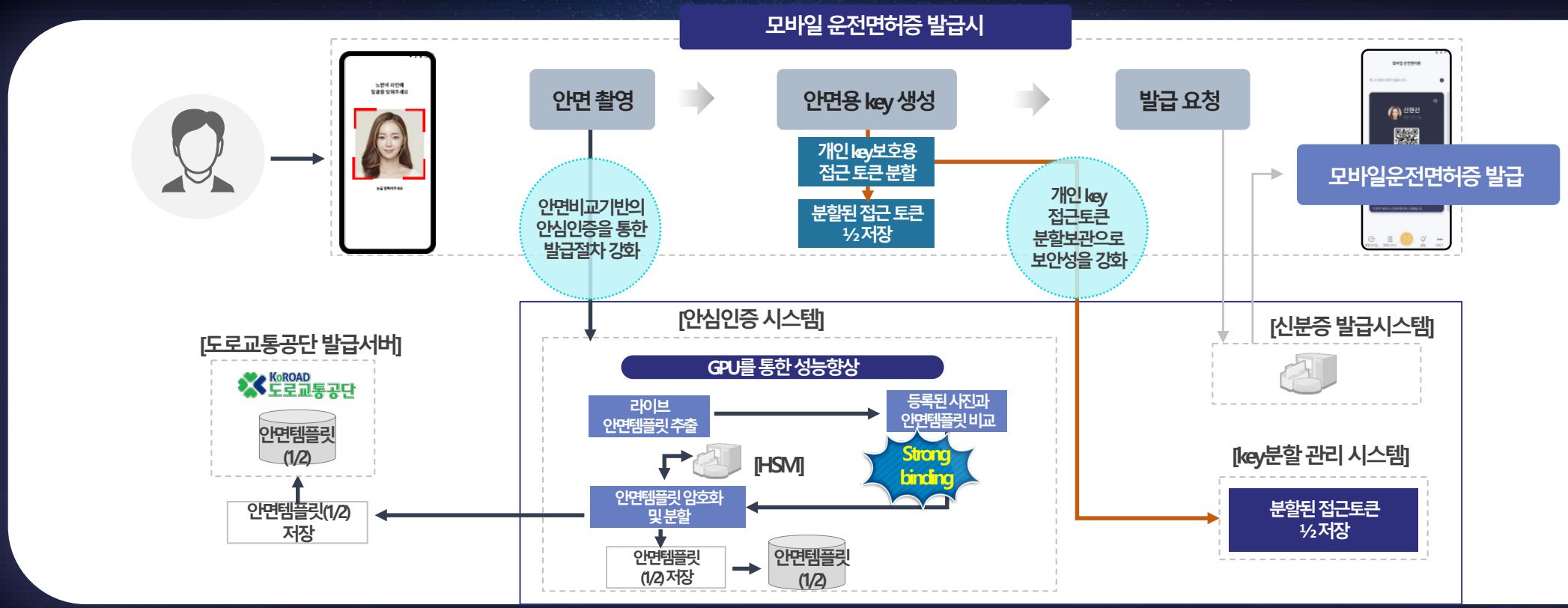
예시

서버기반의 안심인증(안면인증)을 사용하는 이유

- 정당한 소유자가 발급 • 제출했는지를 사전에 등록된 증명사진과 비교•검증하여 강하게 결합할 수 있는 서버기반의 Strong binding 인증 구현

강력한 Strong binding 구현

- 발급주체인 도로공단 발급서버가 발급요청자와 신청자간의 Binding을 직접 검증하지 않고 발급대상인 단말내에서의 비교결과만을 간접 신뢰하고 발급할 수 없음
  사전 등록되고 담당직원을 통해 적절한 사진인지 확인된 정보를 비교
- 검증하여 이용자를 확정짓는 발급서버측 비교 기술을 통해 높은 수준으로 보장이 가능함



05 디지털 신분증 활용 및 관리

예시

언제 어디서나 휴대폰으로 간편한 신원 인증

경찰의 운전면허증 확인 요청시

육안 확인

데이터 제출 필요시

데이터 검증

제출정보

- ☑ 면허번호
- ☑ 면허종별
- ☑ 유효기간

✓ Human Readable의 경우
육안으로 모바일 운전면허증 사진 확인

✓ Machine Readable의 경우 NFC, QR 중
하나의 방식으로 데이터 검증 및 상태 확인

예시

현재 카드형태의 신분증과 동일 효력

은행창구에서 신분증 요청시

육안 확인

데이터 제출 필요시

데이터 검증

제출정보

- ☑ 주민등록번호
- ☑ 이름
- ☑ 주소

✓ Human Readable의 경우
육안으로 모바일 운전면허증 사진 확인

✓ Machine Readable의 경우
NFC, QR 중 하나의 방식으로 데이터 검증

예시

지문 인식률 저하에 따른 편의성 제공

무인민원발급기

데이터 검증

제출정보

- [x] 주민등록번호
- [x] 이름
- [x] 주소

✓ NFC 지원 키오스크는 NFC로 본인 인증

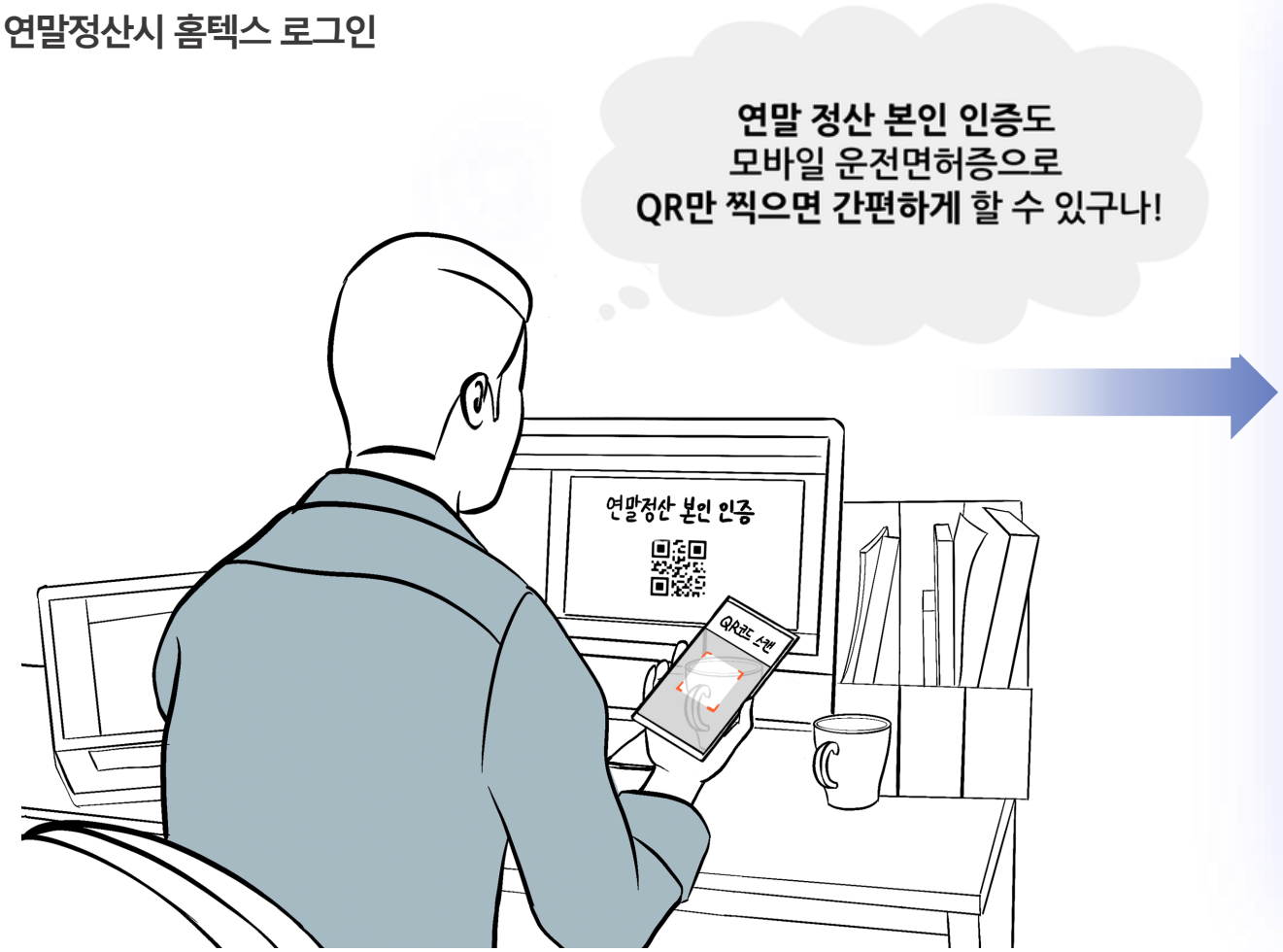
✓ NFC 미지원 키오스크는 QR로 본인 인증

* 사용씬은 변경가능성 있음

예시

본인인증 확인도 자기주권신원인증으로

연말정산시 홈텍스 로그인



✓ 공공포탈 접속시 온라인 본인인증

✓ 로그인 화면에서 QR로 본인 인증

신원증명내역에 대해, 제3자가 알 수 없도록 설계

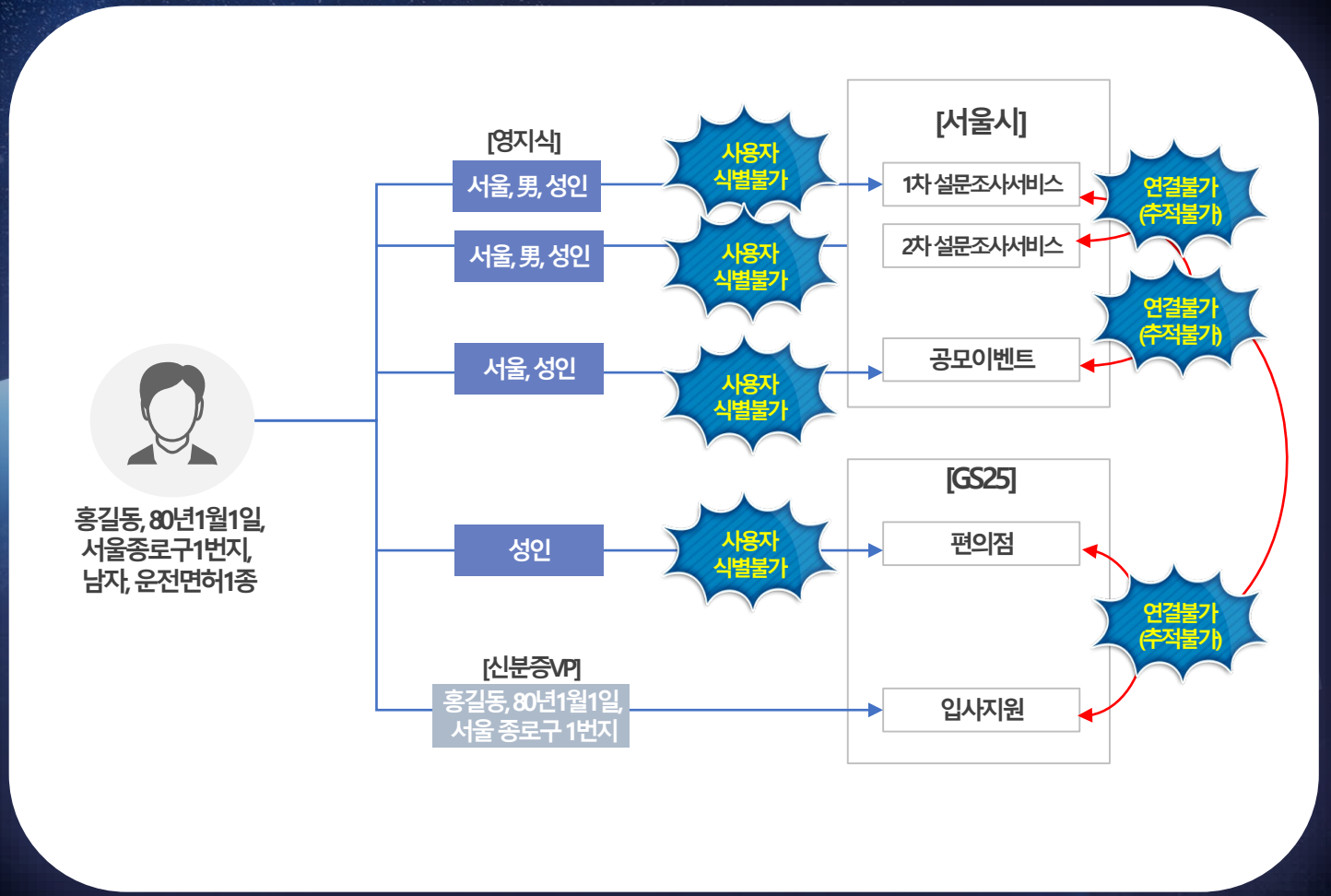
영지식증명(ZKP)를 통한 특정 가능성을 제거

- 동일 도메인 또는 외부 도메인간 관리자의 공모가 있더라도 동일 사용자가 증명한 사실을 알 수 없음
- 또한, 신분증VP의 제출이 있더라도 해당 사용자가 별도로 제출하였던 영지식증명과의 어떤 결부도 시킬 수 없음

Camenisch-Lysyanskaya Signatures 을 사용한 ZKP 특징

- VC소유자임을 증명하는 개인식별, 특정 정보를 포함하지 않음(DID/공개 key)
- VC발급자(Issuer)에게도 노출되지 않는 Master secret을 Blind signature 로 사용자에게 발급
- Non-interactive, with TTP 모델로 구현

■ 영지식용 VC는 Type3 기반으로써 DID와의 연결성을 제거하여 제출한 소유자(Holder)와의 특정가능성을 완전 배제



"국민의 일상을 새롭게 바꾸는 디지털 신분증"

신뢰성

안심하고 쓸 수 있는 든든한 신분증

신분증 특화 안심기술
디지털신분증 생애주기 관리

활용성

생활이 즐거워지는 편리한 신분증

누구에게나 편리한 UX
온/오프라인 신원 인증 환경의 일원화

DID/블록체인 기반 국가 공통 플랫폼 구축


라온시큐업 2021
BEYOND THE DIGITAL WORLD
RAON