

분산신원 기반 학사증명 시스템 (SU 신분증)

DID 팀 (48조)

김수연

이윤성

프로젝트 목표

1. 분산신원 기반 학생증, 성적증명서 발급 및 제시

- 대학교에서 학생증, 성적증명서 등의 증명서를 종이 증명 대신, 분산 신원 기반 자격 증명 형태로 학생에게 발급
- 학생은 이러한 자격 증명을 모바일 지갑앱을 사용하여 외부인에게 제시

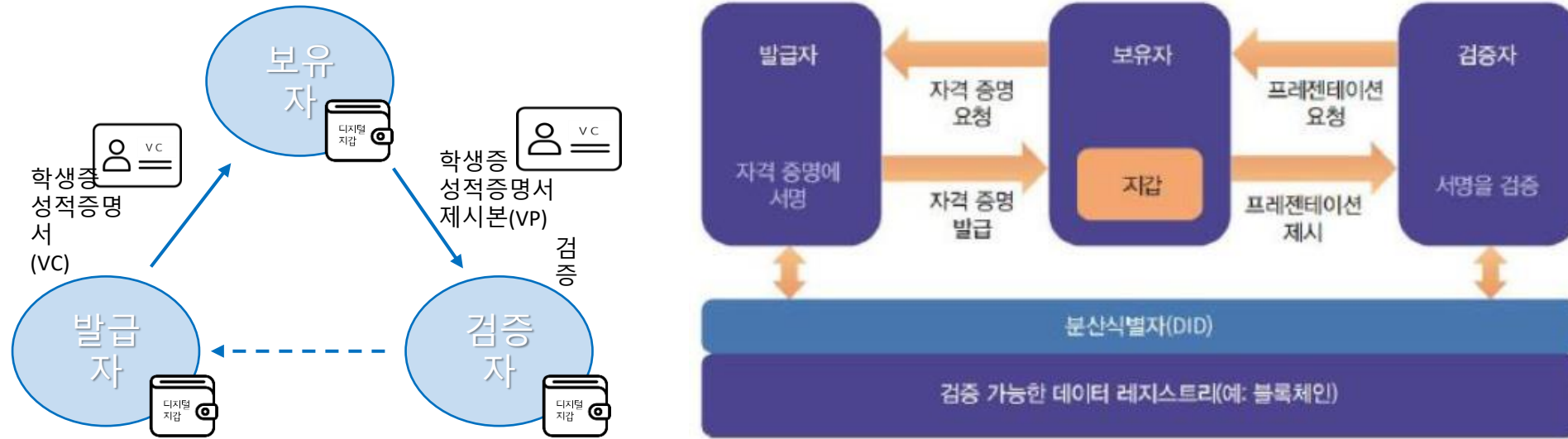
2. 학생증, 성적증명서 검증

- 자격 증명을 제시받은 외부인도 모바일 지갑앱을 통하여 자격 증명을 검증

3. 자격증명 제시시 개인정보 유출 최소화

- 자격 증명 보유자는 개인 정보 유출을 최소화하기 위해 학생증, 성적증명 등 발급된 자격 증명에서 개인정보 일부(주민번호 등)을 가리고 제시하거나 성인 여부만 제시 가능

일반 DID 시스템 아키텍처



- 증명서 발급 앱: 학교 행정원이 학생증, 성적 증명서를 발급하기 위한 앱
- 모바일 지갑 앱(혹은 웹): 발급된 학생증, 성적 증명서를 저장하고 제시하고 검증하기 위한 앱
- VDR(Verifiable Data Registry): 자격 증명의 발급과 제시, 검증 등 전 과정에서 사용되는 공개키와 DID 문서가 저장되는 저장소. 이더리움 등이 블록체인에 저장됨.

필요성

- ♦ 분산 신원(DID) 기술은 DPKI(Decentralized Public Key Infrastructure) 기술을 기반으로 손쉽게 신분증을 발급할 수 있다.
- ♦ 모바일 지갑앱에 저장하기 때문에 자격 증명의 개수가 늘어도 휴대가 간편하다.
- ♦ 육안 검사가 아니라 모바일 지갑앱에서 공개키 기반으로 자동 검증되므로 증명서의 위변조가 사실상 불가능하며, 이를 검증하는 것도 매우 용이하다.
- ♦ 증명서 전체 내용을 제시하지 않고 일부 정보만을 제시할 수 있어 개인 정보 유출을 최소화할 수 있다.

개발 방법

1. 간단한 CLI 기반 DID 예제 코드 분석 및 테스트
 - SSI Korea 포럼에서 제공한 교육 소스 분석
 - CLI 기반 DID 자격증명 발급, 보유, 제시, 검증 클라이언트 검증 기능
 - 이더리움 스마트 컨트랙트 기반 VDR(Verifiable Data Registry) 서버 기능
 - 이더리움2 노드 s/w (RPC server 포함)
2. CLI 기반 학생증, 성적 증명서 DID 자격증명 시스템을 구축 및 테스트
3. GUI 기반 시스템으로 업그레이드 및 테스트

예상되는 문제점 및 대응 방안

- ◆ 분산 신원 기술은 기초적인 부분만 표준화되었고 많은 부분이 표준화되어 있지 않으며 활용할 수 있는 기술자료와 오픈소스가 풍부하지 못하다.
- ➔ W3C에서 현재 진행 중인 표준과 제공되는 코드를 기반으로 구현

모바일 신분증 - 개요

주요 신분증

	주민등록증	전자여권	운전면허증
주관기관	 행정안전부	 외교부	 경찰청
근거법령	주민등록법	여권법	도로교통법
형태	플라스틱 카드	IC 칩이 탑재된 전자여권	플라스틱 카드 또는, IC운전면허증

정부기관이 근거 법령에 의해 발급함으로써
개인의 신분을 공식 증명하는 문서

모바일 신분증 - 개요

그러나, 플라스틱 신분증은...

오프라인




금융기관
공공기관

위변조 및 도용 우려

실물카드로 신원확인

- ✓ 개인정보가 공개된
실물 플라스틱 카드로 신원 확인
- ✓ 상시 휴대 불편, 훼손
- ✓ 위 변조 및 도용 우려 상존

온라인



인터넷뱅킹
공공 웹사이트
쇼핑/커머스

스마트폰 인증
소셜 인증
공동 인증서

서비스 제공기업

개인정보유출 취약

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

모바일 신분증 - 개요

모바일 신분증 플랫폼



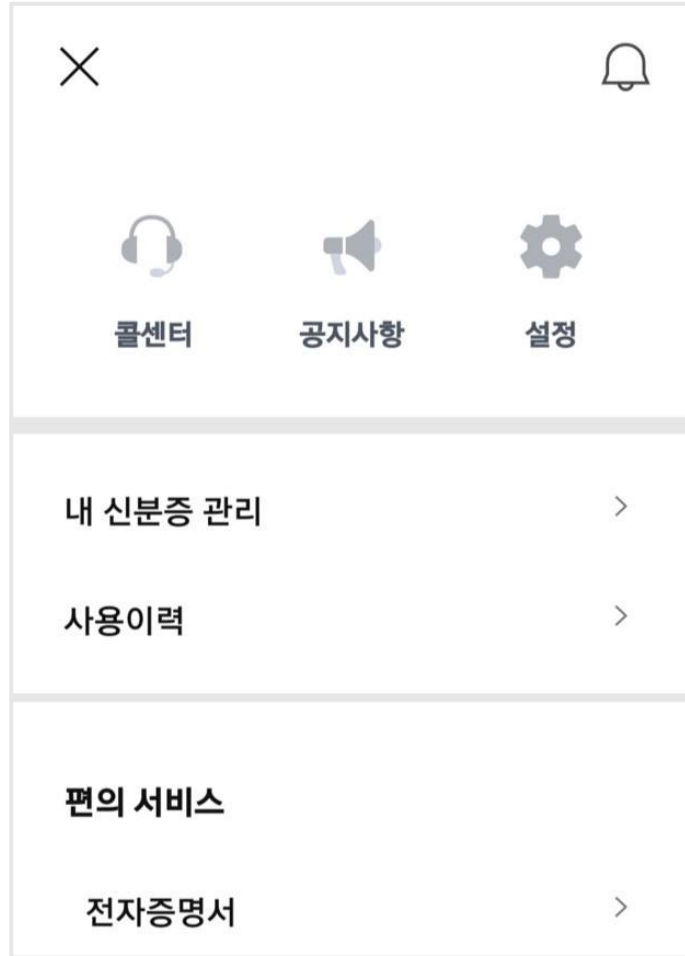
분산신원증명(DID) 블록체인 플랫폼

국가 신분증으로서
공신력 보장

안전하고 신뢰할 수 있는
공통 플랫폼 구축

유용하고 쓰임새 많은
온라인 편의 서비스

모바일 신분증 - 주요 기능



모바일 신분증(운전면허증) – 검증 방법

(육안확인)



(검증앱)



(별도 검증시스템 구축)

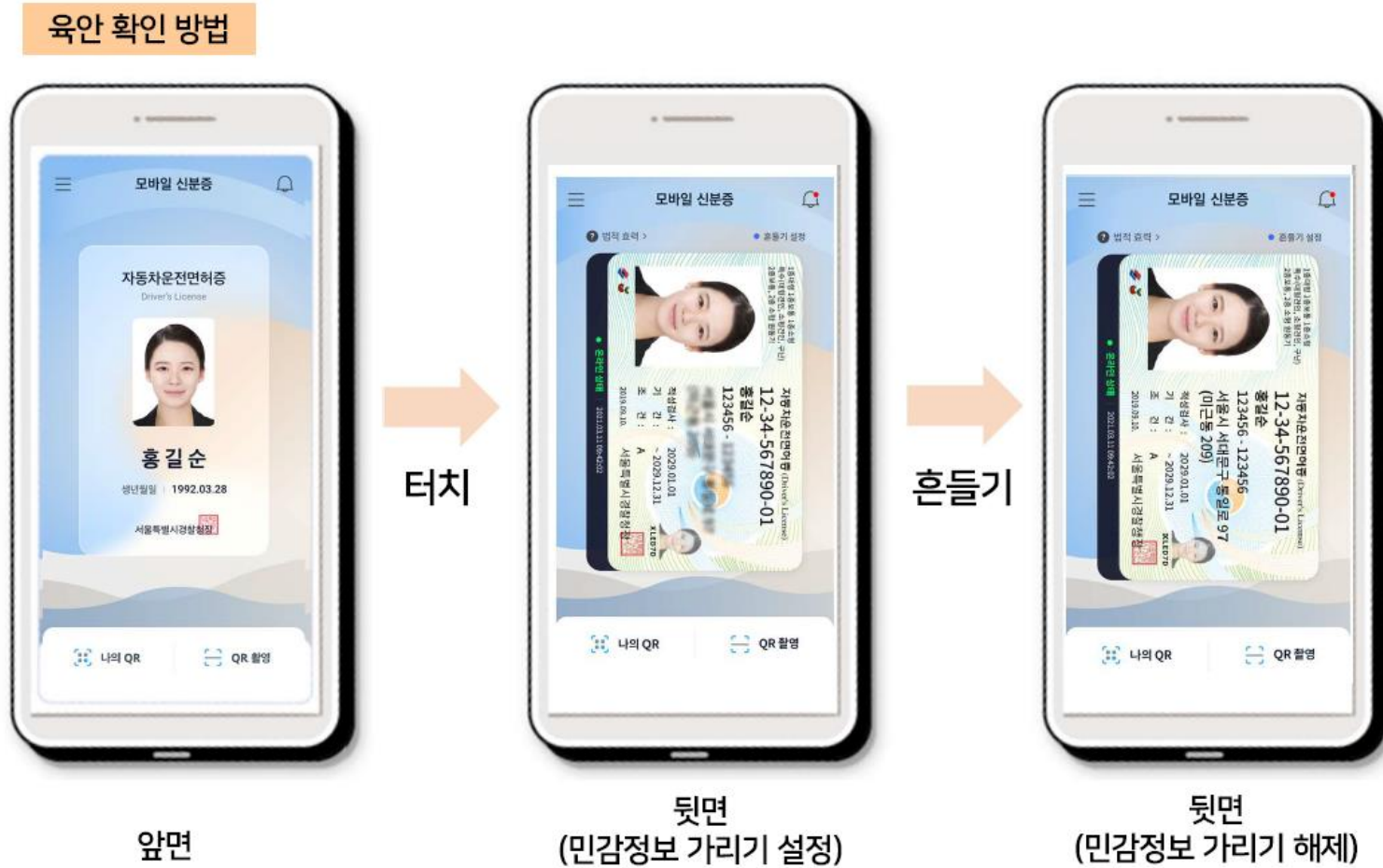


1. 모바일 운전면허증
보여주기

2. QR코드 보여주기

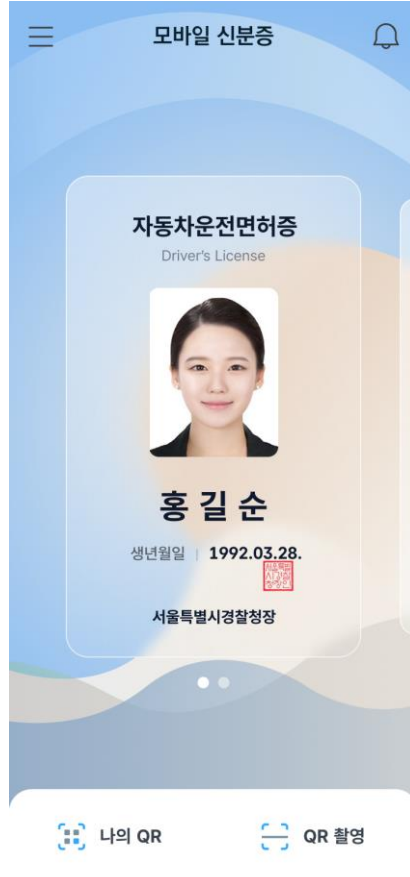
3. QR코드 촬영하기

모바일 신분증(운전면허증) - UI - 육안 확인



모바일 신분증(운전면허증) – UI – QR 제시

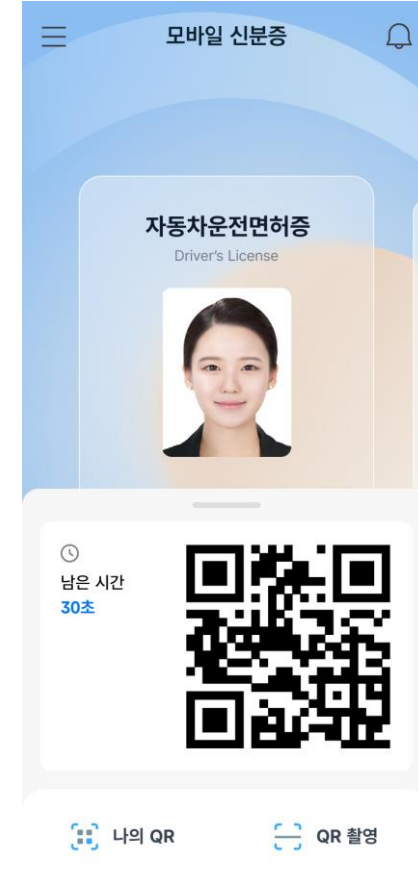
모바일 신분증 (메인메뉴)



법적 효력 표시



모바일 신분증 QR 제시



모바일 신분증(운전면허증) - UI - 온/오프라인

온라인 상태, 블러 처리



온라인 상태, 전체 표기



오프라인 상태, 블러 처리



오프라인 상태, 전체 표기



모바일 신분증(운전면허증) - 기능별 시나리오

[설치]

1. 앱 설치
2. 권한 허용
3. 본인 인증
4. 비밀번호 및 생체인증 등록

[발급]

1. 서비스 약관 동의
2. 신청서 작성 - 이름, 주민등록번호 입력
3. IC 신분증(운전면허증) 준비
4. NFC 기능 활성화
5. IC 신분증(운전면허증) 비밀번호 입력
6. IC 신분증(운전면허증) NFC 태그
7. 3~6 과정 대신 운전면허시험장에서 QR 발급

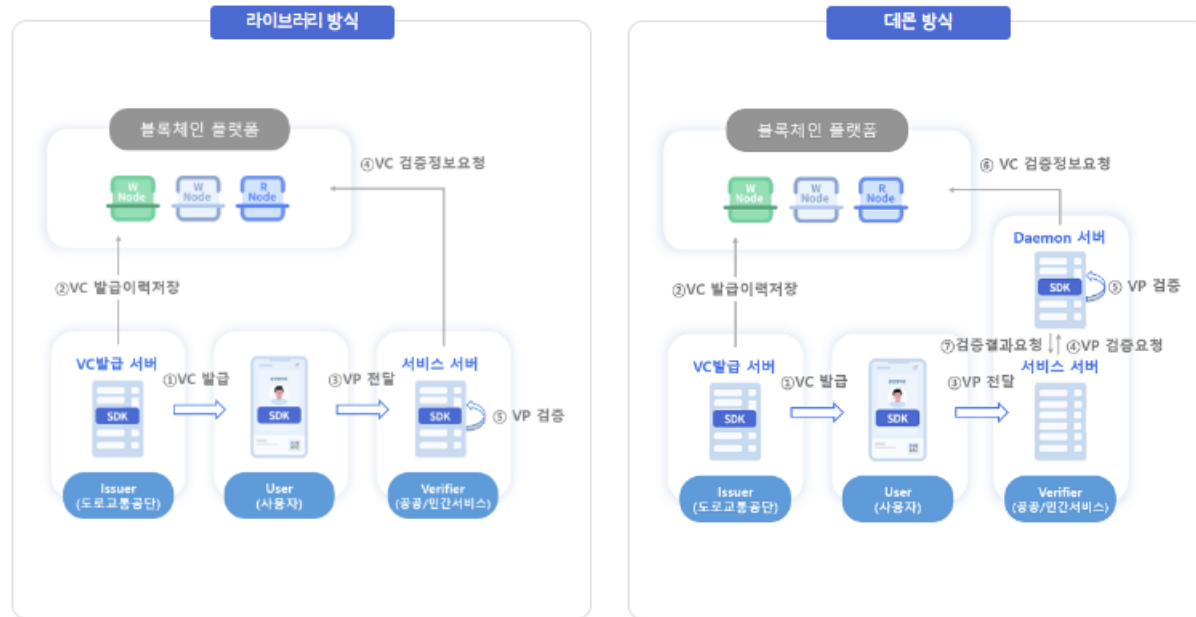
[사용]

1. 검증 앱 실행
2. 요청정보 선택
3. 신분증 소지자가 QR 제공
4. 신분증 QR 촬영
5. 신분증 소지자가 요청정보 확인 및 제공 승인
6. 진위확인된 신원정보 확인

모바일 신분증(운전면허증) – 시스템 구성도

연계 방식

분류	설명
라이브러리 방식 (JDK 1.7 이상 필수)	· 이용기간 서비스에 개발 적용하여 모바일 운전면허증 신원 및 자격 검증하는 방식
대문방식	· API방식으로 연계되어 개발언어에 영향을 받지 않아 보다 쉽게 개발이 가능한 방식



모바일 신분증(운전면허증) – 인터페이스 방식

인터페이스 방식

분류	설명
QR-MPM	· 검증자가 QR을 표출하고 이용자가 QR촬영하여 신원 및 자격을 검증하는 방식
App2App	· 이용기관 서비스 앱과 모바일 신분증 앱을 연계하여 신원 및 자격을 검증하는 방식
QR-CPM	· 이용자가 QR을 표출하고 검증자가 QR촬영하여 신원 및 자격을 검증하는 방식
PUSH	· PUSH 메시지를 통해 신원 및 자격을 검증하는 방식

NO.	분류	사용자 모바일 인터페이스				모드			
		QR		입력	APP	indirect (응대장치)	direct (SP서버)	proxy (중계서버)	P2P
		표출	스캔	키보드	APP호출				
1	QR-MPM direct mode		●				●		
2	QR-MPM proxy mode		●					●	
3	App2App direct mode				●		●		
4	App2App indirect mode				●	●			
5	QR-CPM proxy mode	●						●	
6	PUSH			●					

모바일 신분증(운전면허증) - 특징

- ◆ 장점

- ◆ 법적 효력이 있는 신분증 제시 및 검증 가능 (육안, QR, NFC/BLE)
- ◆ 보안성 강화
 - ◆ 모바일 신분증 QR 코드 값
 - ◆ 200자리의 문자열 (검증 정보가 충분히 포함된 것으로 추정됨)
 - ◆ eyJjbWQiOiIxMjAiLCJob3N0Ijoid3NzOi8vbXZhdhMDlubW9iaWxlaWQuZ28ua3I6OTA5MC9wcm94eVNlcnZlcilslm1vZGUlOiJwcm94eSIsInRyeGNvZGUlOiIyMDI0MDUyMjE2MjkzMjE2MEMwQzQxNjM0IiwidHlwZSI6Im1pcCIsInZlcnNpb24iOiIxLjAuMCJ9

- ◆ 보완할 점

- ◆ 증명서 미지원

모바일 공무원증 - 개요

- ◆ 모바일 공무원증
 - DID 기술이 적용된 자기주권 신원증명의 모바일 신분증
 - 신원 주체인 개인이 소유 및 이용 권한을 가짐
 - ↔ 중앙집중식 신원증명과 대조됨
 - 소유자는 스마트폰에 신분증을 발급받아 보관 후,
신원 확인 요청시 판단 하에 정보 제공 여부 결정
 - 신분증 사용 이력은 개인의 스마트폰에 저장되어 본인만 확인 가능
 - ↔ 중앙서버에는 저장되지 않음

모바일 공무원증 - 기능 목록

기능 구성

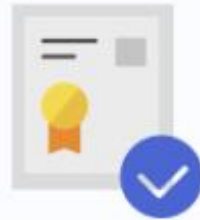
모바일 공무원증은 청사출입, 시스템 로그인 및 기타 다양한 신원인증 서비스를 제공합니다.



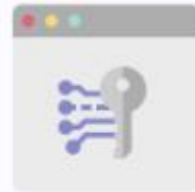
모바일 공무원증 - 주요 서비스



신원 증명



증명서 발급



시스템 로그인



청사 출입



도서 대출

모바일 공무원증 - 기능 목록

[발급]

1. e-사람에서 발급신청
2. 부서장 결재
3. 발급신청 확인 및 처리
4. 발급준비 SMS 수신
5. 설치 URL 통해 앱 다운로드
6. 비밀번호 설정
7. 본인확인 및 이용동의

[Help]

1. 알림
2. 권한설정
3. 환경설정

[APP 로그인]

[QR 스캔]

1. 신분증 앱으로 QR 스캔
2. 웹 사이트 방문

[QR 제출]

1. 검증 앱 실행
2. 요청정보 선택
3. 신분증 소지자가 QR 제공
4. 신분증 QR 촬영
5. 신분증 소지자가
요청정보 확인 및 제공 승인
6. 진위확인된 신원정보 확인
7. 출입

[NFC 기능]

[신분증 관리]

1. 발급된 신분증 목록 확인
2. 삭제하기

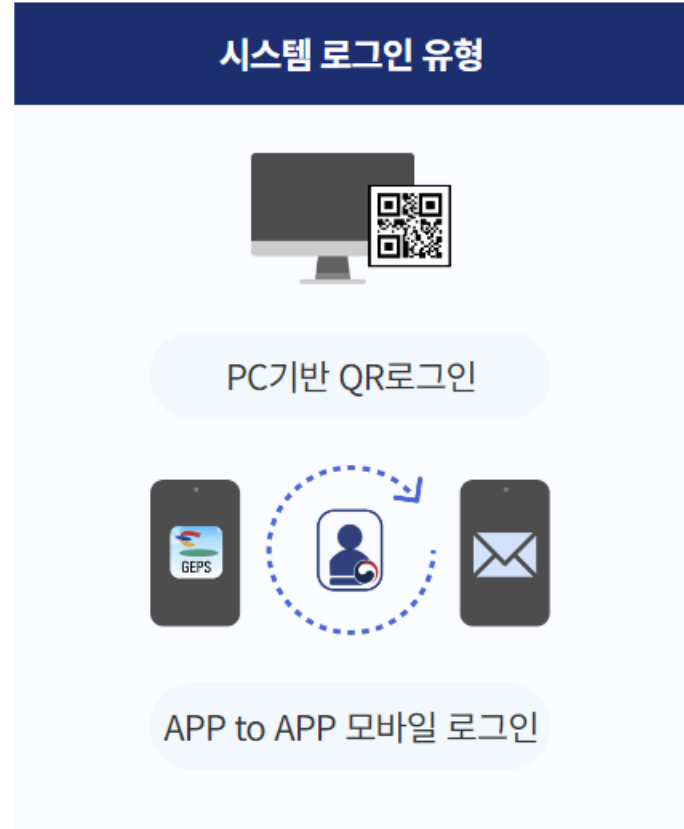
[증명서 관리]

1. 증명서 목록 조회
2. 제출하기
 - 2-1. 해당기관 QR 스캔
 - 2-2. 항목 선택
 - 2-3. 신분증 제출

[사용기록]

1. 시간순/사용처별 보기
2. 저장하기

모바일 공무원증 - QR 스캔 기능



모바일 공무원증 – 청사 출입 기능 (NFC/BLE)

청사 출입 소개

정부청사 출입은 스마트폰만으로도 세종과 서울 청사의 게이트 및 사무실을 출입할 수 있는 서비스입니다



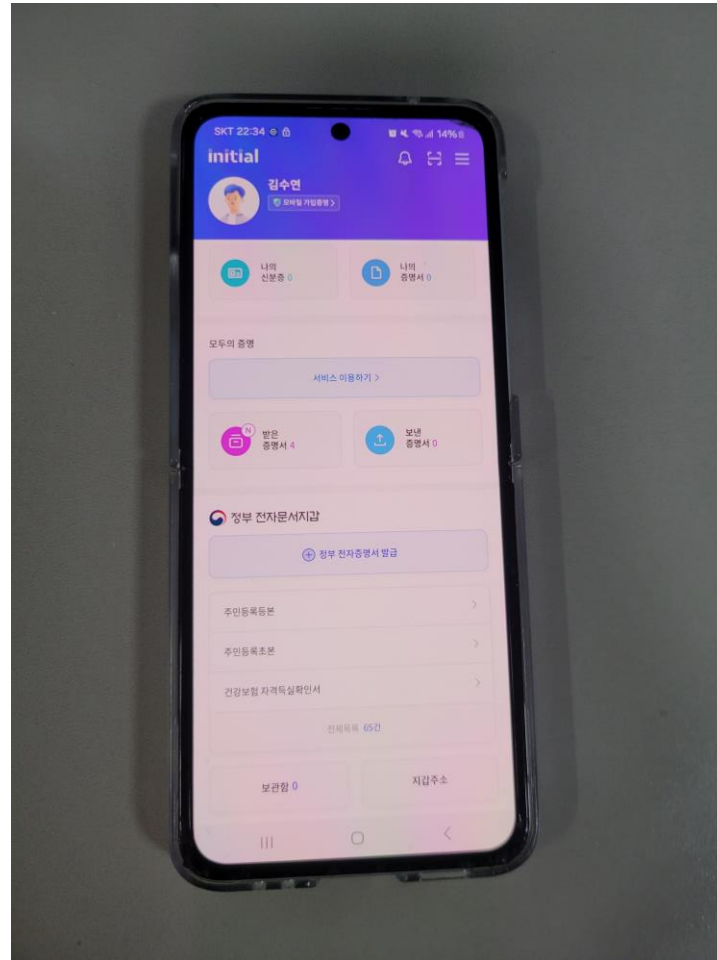
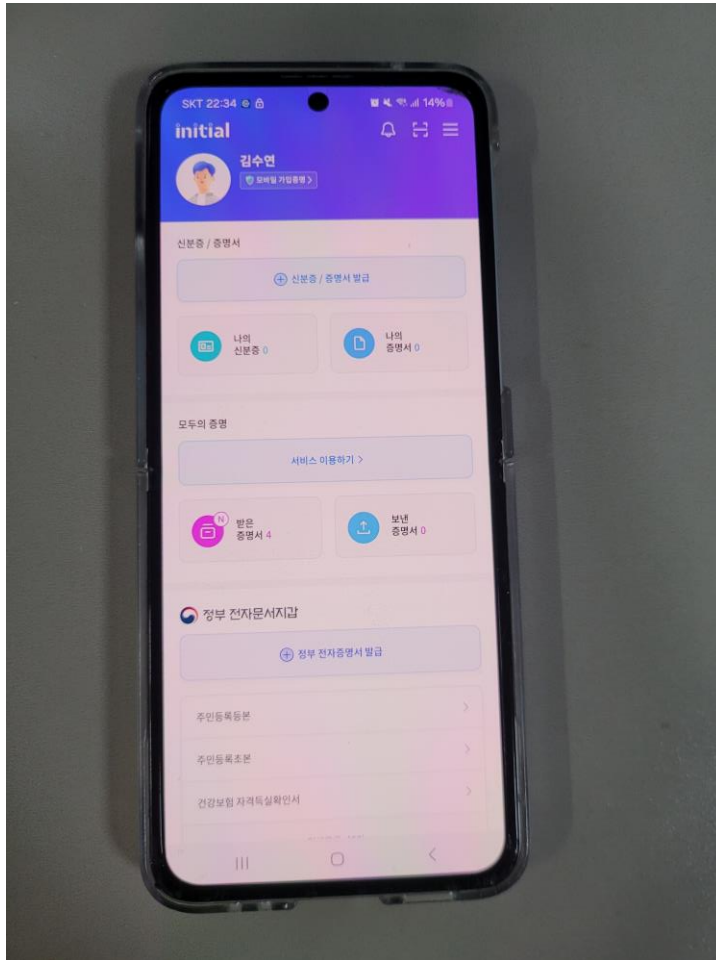
- 안드로이드폰 : NFC활용
- 아이폰 : BLE활용

※ 출입 가능 구역은 공지사항 참조

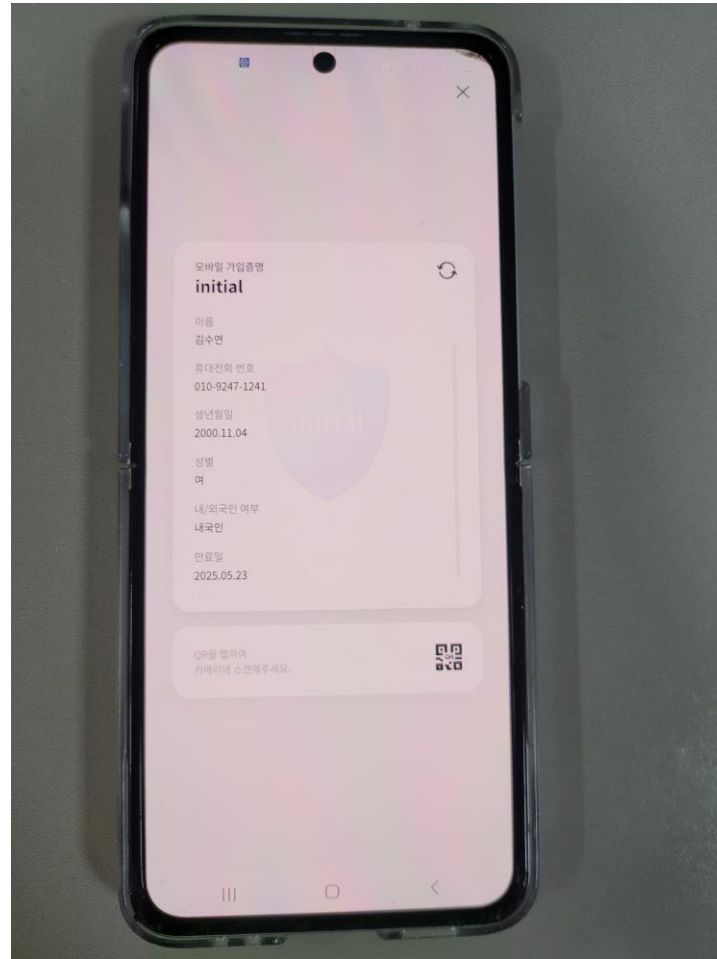
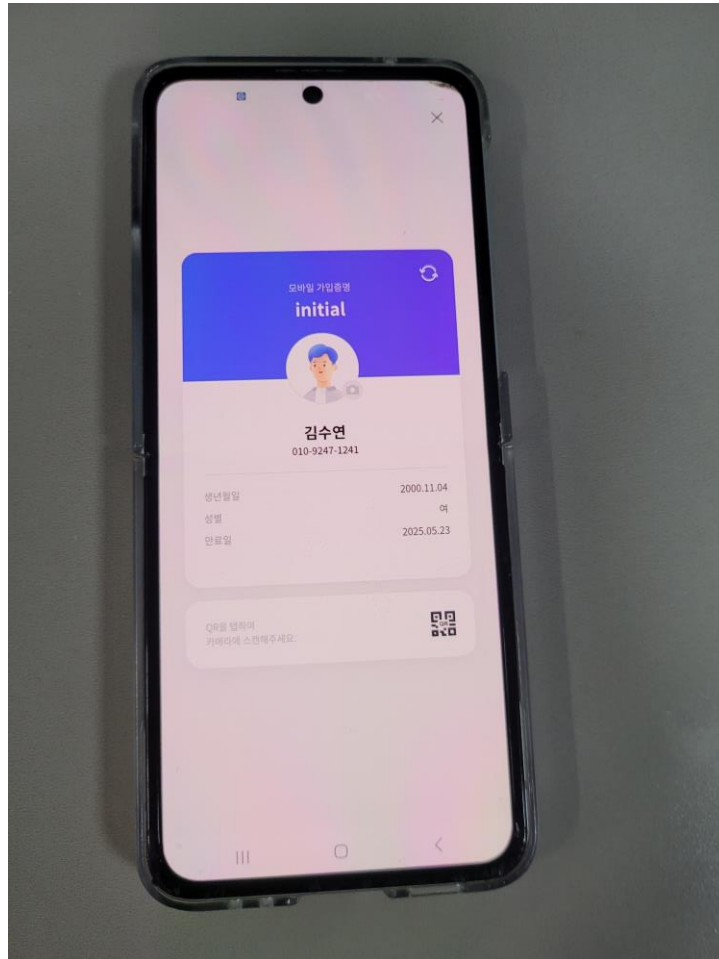
모바일 공무원증 - 특징

- ◆ 법적 효력 있는 신분증 제시 가능
- ◆ 보안성이 약해보임
 - ◆ 일반인은 육안 확인만 가능
 - ◆ QR 검증 모바일 앱 기능이 없음
- ◆ 정부 시스템 내부에서만 신분증 검증 가능

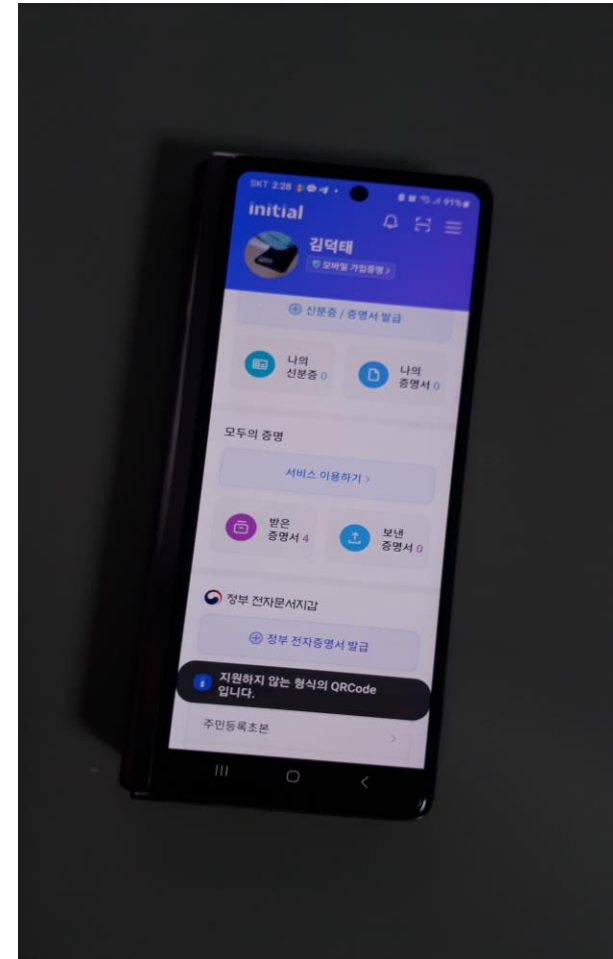
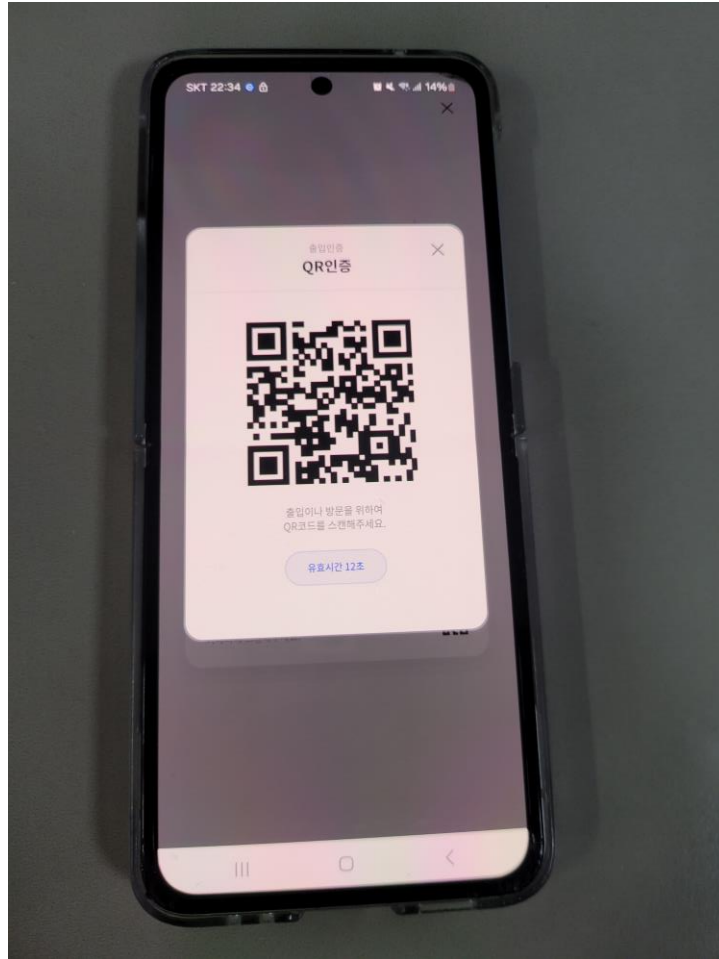
SKT 이니셜 - 주요 기능



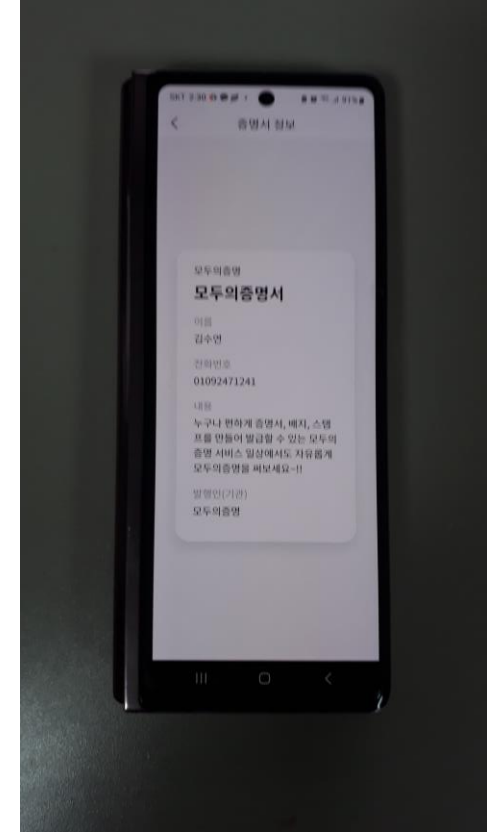
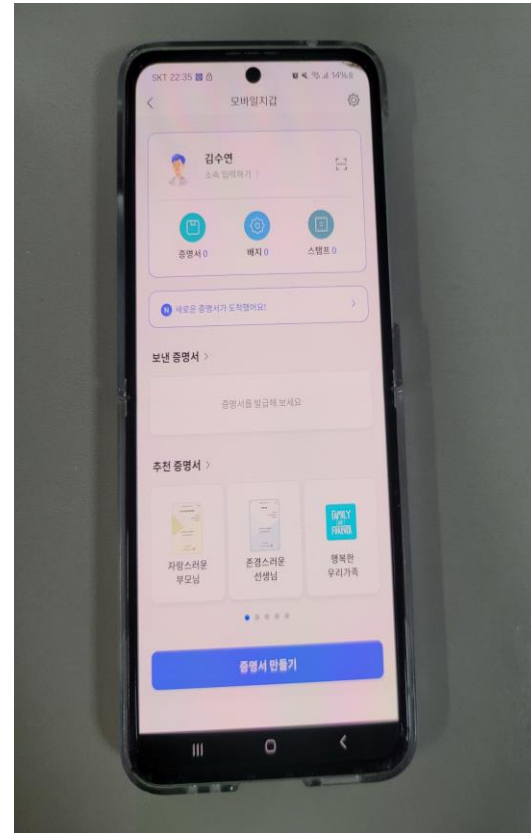
SKT 이니셜 - 가입 증명 육안 제시 화면



SKT 이니셜 - 가입 증명 QR 제시 및 검증 화면



SKT 이니셜 - 모두의 증명 QR 제시 & 검증



SKT 이니셜 - 특징

- ◆ 모두의 증명 서비스만 QR 제시 및 검증 가능
 - ◆ 누구나 증명서 종류별 발급 및 검증 가능 (확인증, 상장/표창장, 인증서, 신분증)
 - ◆ 기본증명인 모바일 가입증명, 보관된 신분증/증명서의 QR 제시 및 검증 미지원
- ◆ 민간 신분증 발급 요청 및 보관
 - ◆ 대학 신분증 및 교우증, 진료카드, initial 학생증, 반려동물확인증 등
- ◆ 민간 증명서 발급 요청 및 보관
 - ◆ 대학교 졸업증명서, 졸업예정증명서, 성적증명서, 출입권한증명, 영수증 등
 - ◆ QR 보안성이 충분한 것 같음
- ◆ 정부 전자증명서 발급 요청 및 보관 (주민등록등본 등)
- ◆ 정부 신분증 QR 검증

SKT 이니셜 - 특징

♦ 가입증명의 보안성 취약

- ♦ SKT 이니셜 가입증명 QR 코드 값 (QR 드로이드 앱으로 확인)
 - ♦ 01092471241200011042024052014540815
 - ♦ 전화번호 + 생년월일 + 날짜&시각을 이어붙인 단순한 구조

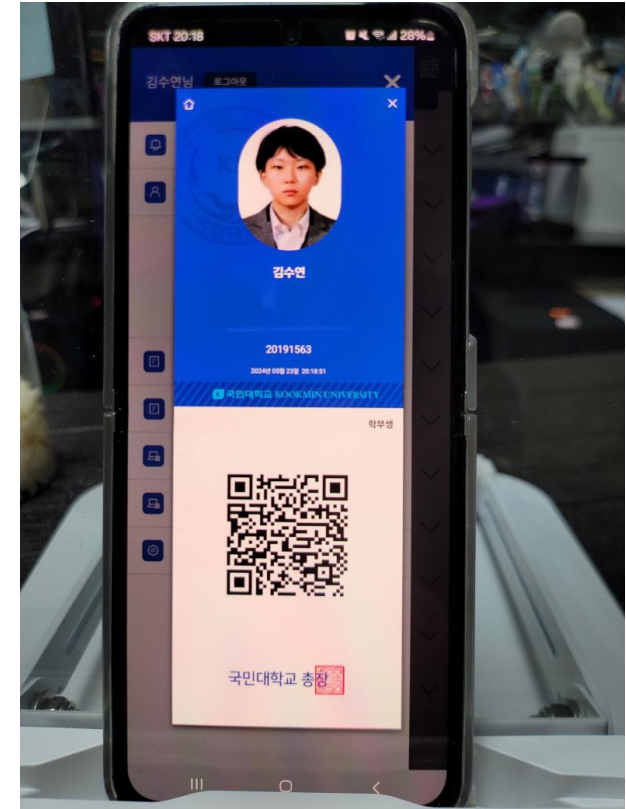
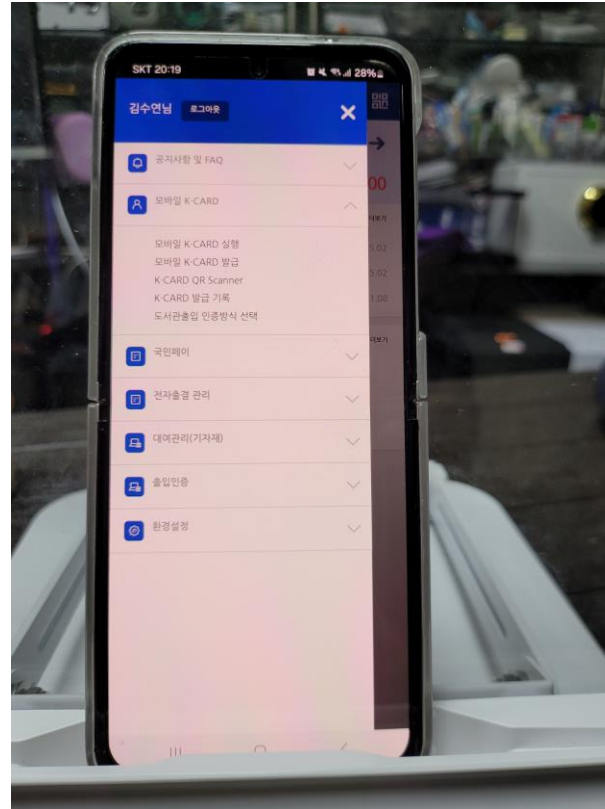
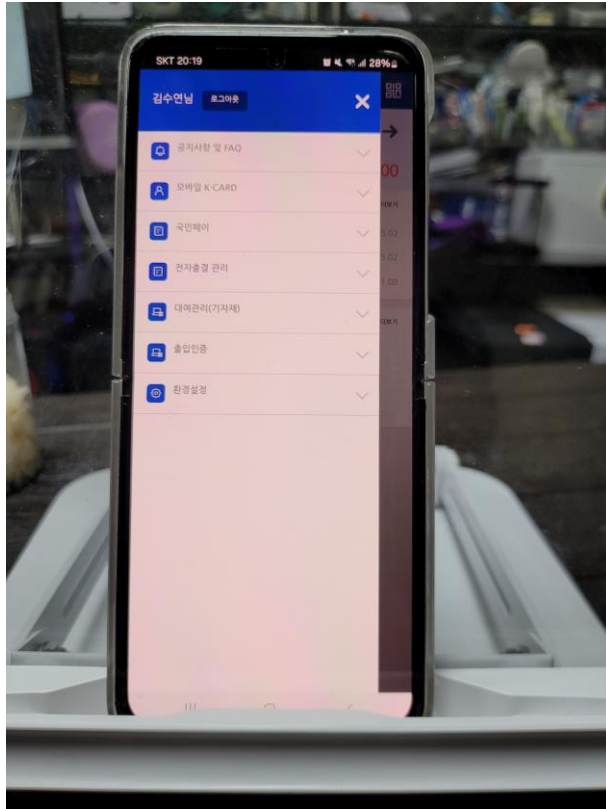
♦ 증명서의 보안성 강화

- ♦ 모두의 증명서 QR 코드 값
 - ♦ 248자리 문자열

6889ca2df22866ee198d3527d683e6405199859e37350e1b557a147124b6fe9faef4ab9f0946159b2922cd50fff393d08f0761b930c4e2274923ffd0b0d9dece6427ecac9f7e342df4ab7247bc956eb58de056a00f694e7f86a6312f1caa6bade7e93184a03344d220f613e493c3ff8deb4a13854cced78f5f22b5ebca28591df83a3e6d33f1ac96ac3644cfa223efb4872ba19af99cfb41907631e8b0451222fa1ba1b70f2e8520c054163073d68155747eb509202e95ef95d3a7a0f84316015cb2a0608bd64ac5ac59e823a2145d3a4e2c75b0d67661617710c7260266f24853cde011a52ba05f618e52c52227e9c8a19e25fc857f2164da87065409d525124c8ac5cce502e97627d908d202d0b38c0eee4198825668137385799711a51b3cac2ba0144622a23cff303db87e57afd4da439a14902306a21987d2f43fb950abe12a4487fc3208d4603907e9f551f2e48c63e3a2134447533f135378cfc44c696dac7809e078712ebc32c565cbb0ba13ca0554196b77eab4c71c4bad9ff9cbb3462b281573cef45633a815f392d501fbb8b6405d2dee7a741280279bf5f7f6ba0afbb8d9f27113a7b6ed1c8f135f5162e932aa174297b6ce51b0062e5858d567c62af08d82a2d72b9688374cd4f12fe0cce769932ba47a747282501de931e6c0

♦ 이니셜 학생증에 QR 제시 적용 안 됨

모바일 K-card – 주요 기능



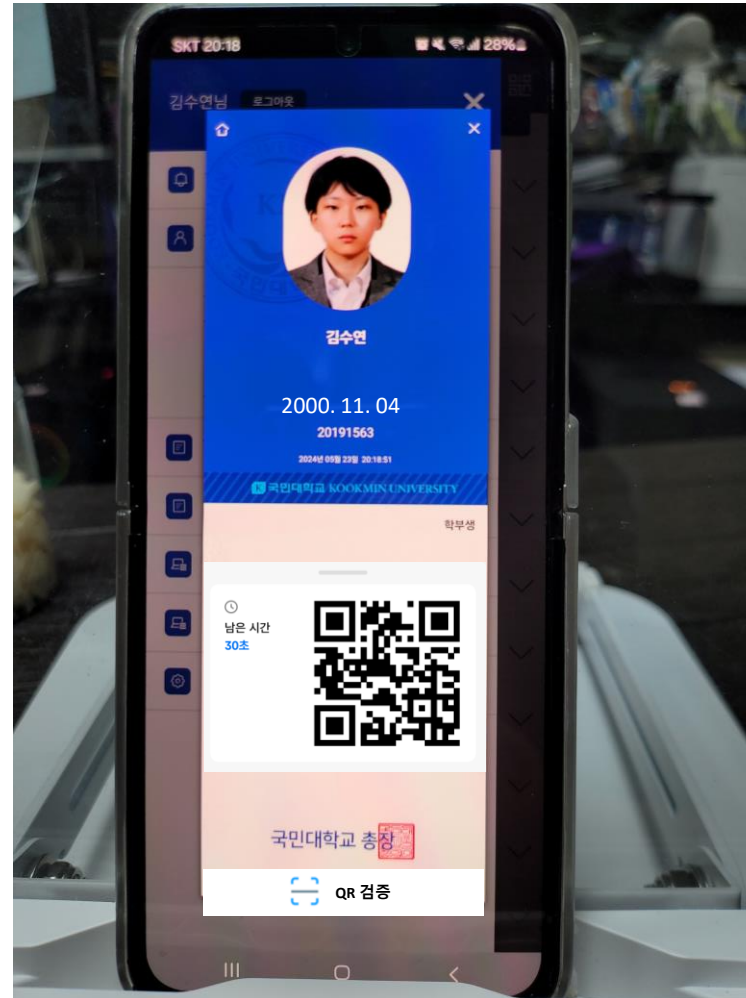
모바일 K-card – 특징

- ◆ 검증 가능한 학생증 제시
- ◆ 출석/출입, 금융서비스 연동
- ◆ 법적 효력 없음
 - ◆ 외부에서 사용하기 어려움
- ◆ 교내 및 연계된 서비스만 이용 가능
- ◆ K-card QR 코드 값
 - ◆ 64자리 문자열 (보안이 취약해보임)
 - ◆ fe5f946d2f5a4b2504b3344a6740882742d3b5503c96b3e48c52100db4740a73

본 프로젝트의 특징

- ◆ 주요 기능
 - ◆ 학생증, 성적증명서 발급 요청 및 보관
 - ◆ 학생증 제시 및 QR 검증
 - ◆ 성적증명서 제시 및 QR 검증
 - ◆ 민감정보 숨김/표시
- ◆ K-card 대비 장점
 - ◆ QR 코드를 앱으로 교내 구성원 및 외부에서 신뢰성 있게 검증 가능
 - ◆ 국민대 학생 여부, 성인 여부 확인 가능
 - ◆ 선택적 개인정보 제시
 - ◆ 성적증명서 열람, 제시 및 신뢰성 있는 제 3자 검증 가능

UI 설계 1



UI 설계 2

학생증 VP
제시 화면



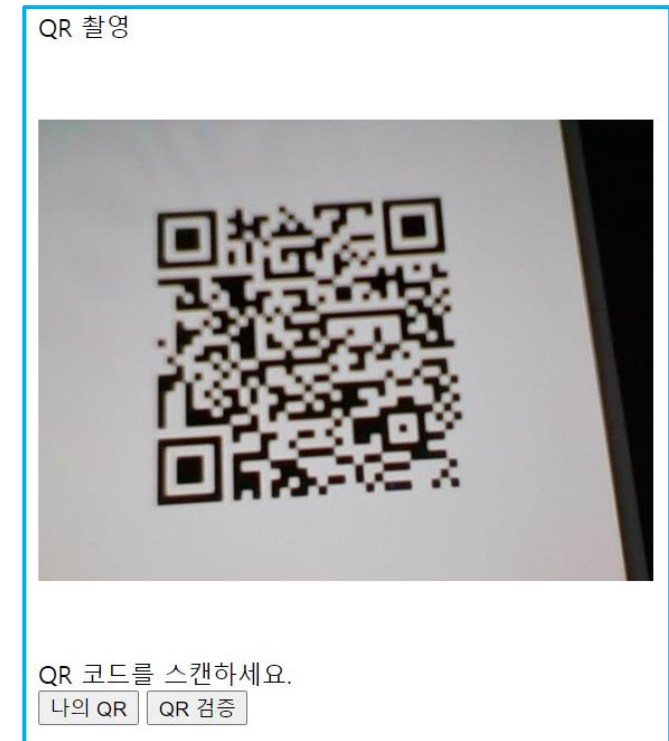
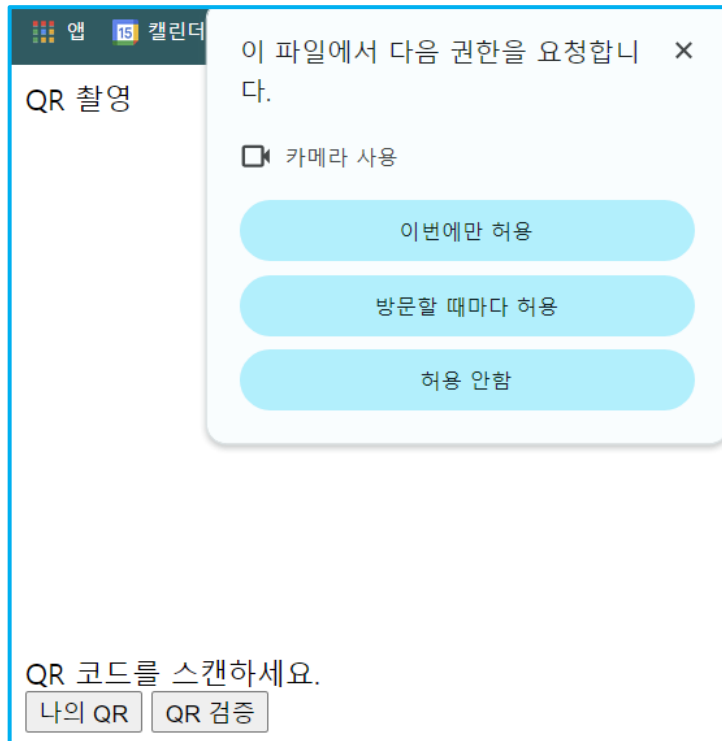
성적증명서 VP
제시 화면



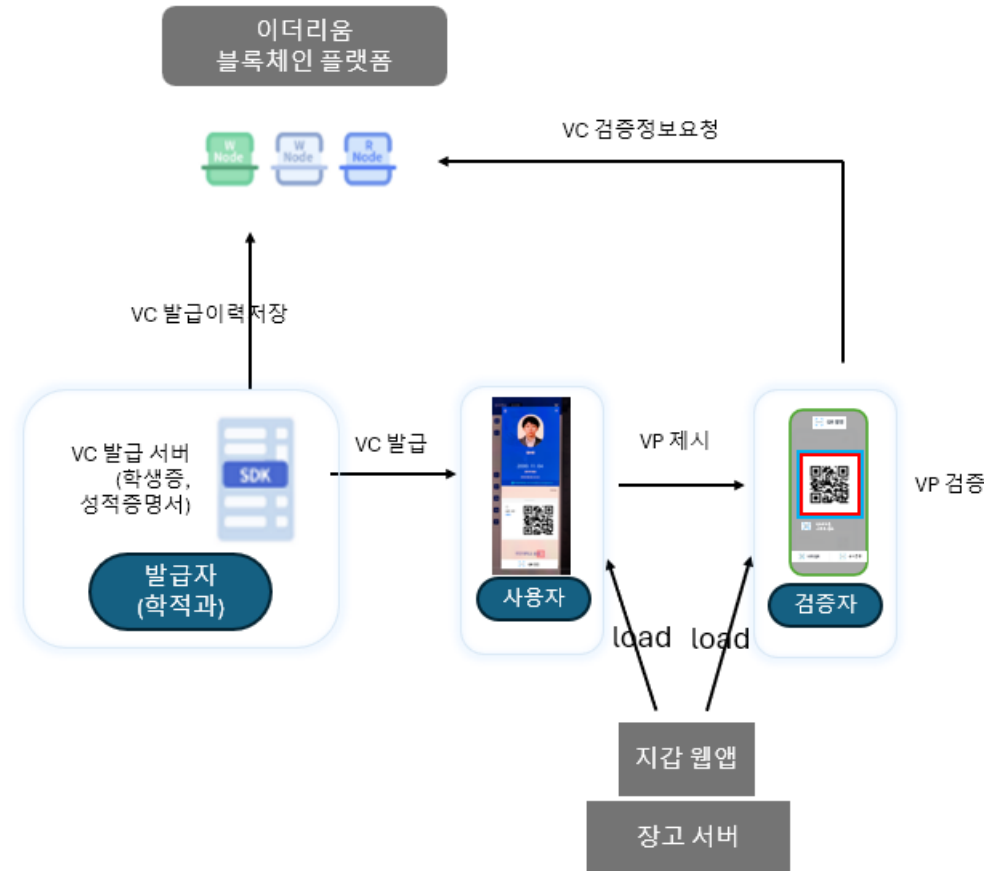
VP 검증 화면



UI 구현



시스템 구성도



신분증 앱 구현

- 언어: 자바스크립트, 파이썬
- 프레임워크: 장고
- QR 생성 js 라이브러리: qr-code-styling.js
- QR 인식 js 라이브러리: Html5-QRCode
- PWA 기술 (웹 스토리지) 적용 (예정)

VDR(Verifiable Data Registry) 구현 (예정)

- W3C DID 표준
- 이더리움 2 프라이빗 네트워크 노드 3개 구축
- 이더리움 스마트 컨트랙트로 VDR 구현

향후 과제

- 신분증, 증명서 자체 발급(만들기) 및 보관
 - 회원증, 영수증, 차용증, 추천장, 상장
- 인앱 생체인증/PIN 번호 설정
- 신분증 앱에서 QR 코드 스캔하여 신원 검증
 - QR코드 스캔을 통한 웹 사이트 로그인
 - QR 코드 제시와 정반대
- NFC/BLE 기능을 통한 신원 검증
 - 출입 통제
- App2App 신원 검증
- 사용기록 저장 및 보관
 - 시간순, 사용처별 보기
- 민간 신분증 및 증명서 발급 요청 및 보관
- 정부 신분증 및 증명서 발급 요청 및 보관
- 신분증, 증명서 관리
 - 제출하기
- 검증 시스템 인터페이스