모바일 신분증 적용 “OpenDID”, 오픈소스 개발과정과 앞으로의 계획

2025.03.25

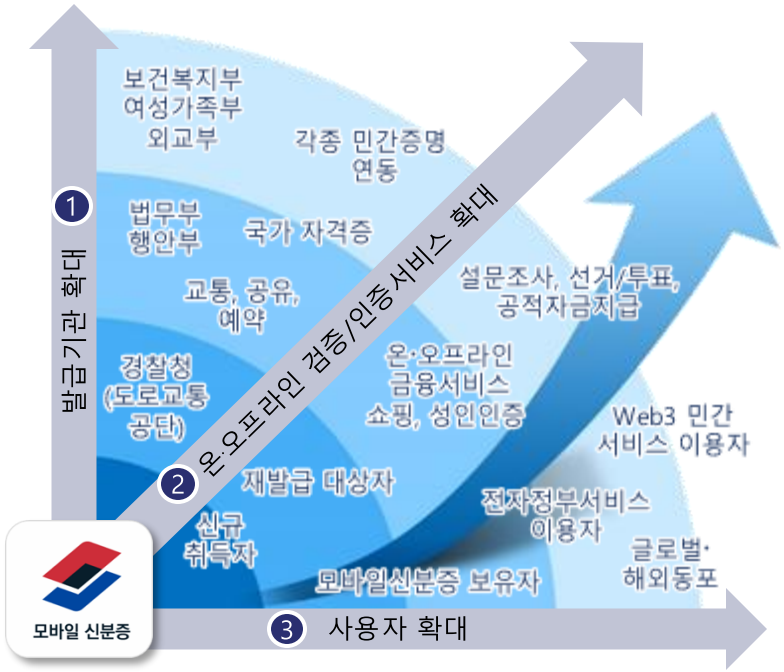
라온시큐어 이미경 팀장

2025/03
Ver. 1.0

목차

01 모바일 신분증

- 모바일 운전면허증을 시작으로, `25년 현재, 모바일 주민등록증, 외국인등록증 등 발급 진행 중



모바일 운전면허증 (2022)

모바일 국가보훈등록증 (2023)

재외국민신원확인증 (2024)

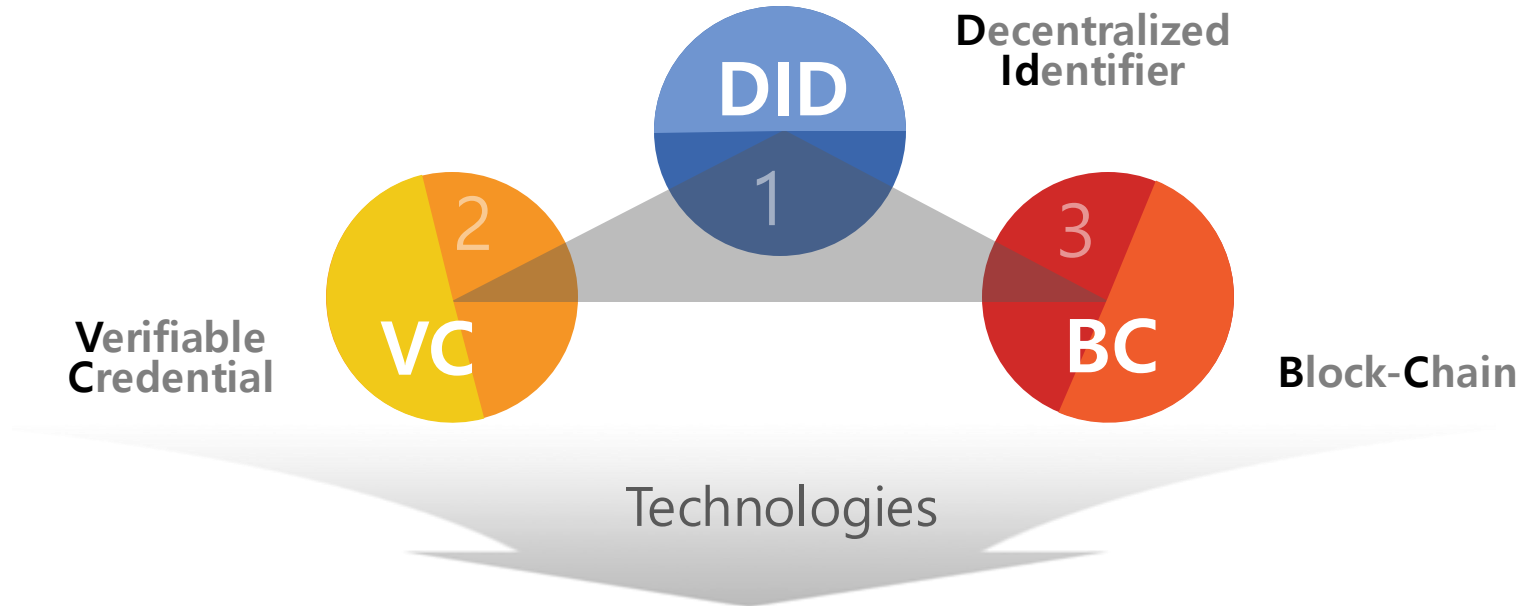
모바일 주민등록증 (2024)

모바일 외국인등록증, 국내거소신고증, 영주증 (2025)

모바일 국가기술자격증 (2025)

* 모바일 장애인등록증 2025년 하반기 서비스 예정

모바일 디지털지갑에 국가ID 신분증(VC)를 암호화하여 저장하며, 이용처 제출 시 정부 DID 블록체인을 통하여 신원증명이 가능한 자기주권 신원증명체계

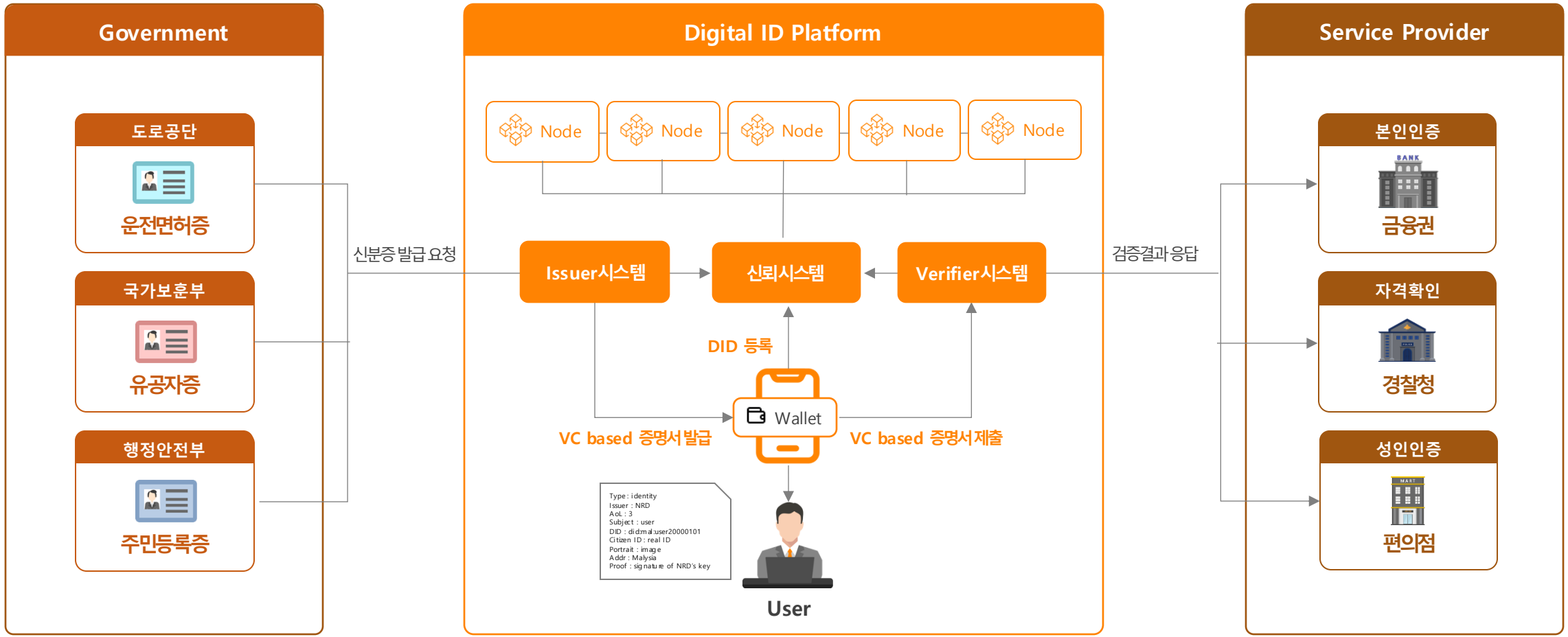


블록체인 기반 탈중앙화(DID) 기술을 활용한 한국형 모바일 신분증 플랫폼

Security O | Convenience O | Privacy O

02 Open DID 기술 개요

Open DID 개요도



DID(Decentralized Identifier)는 무엇인가?

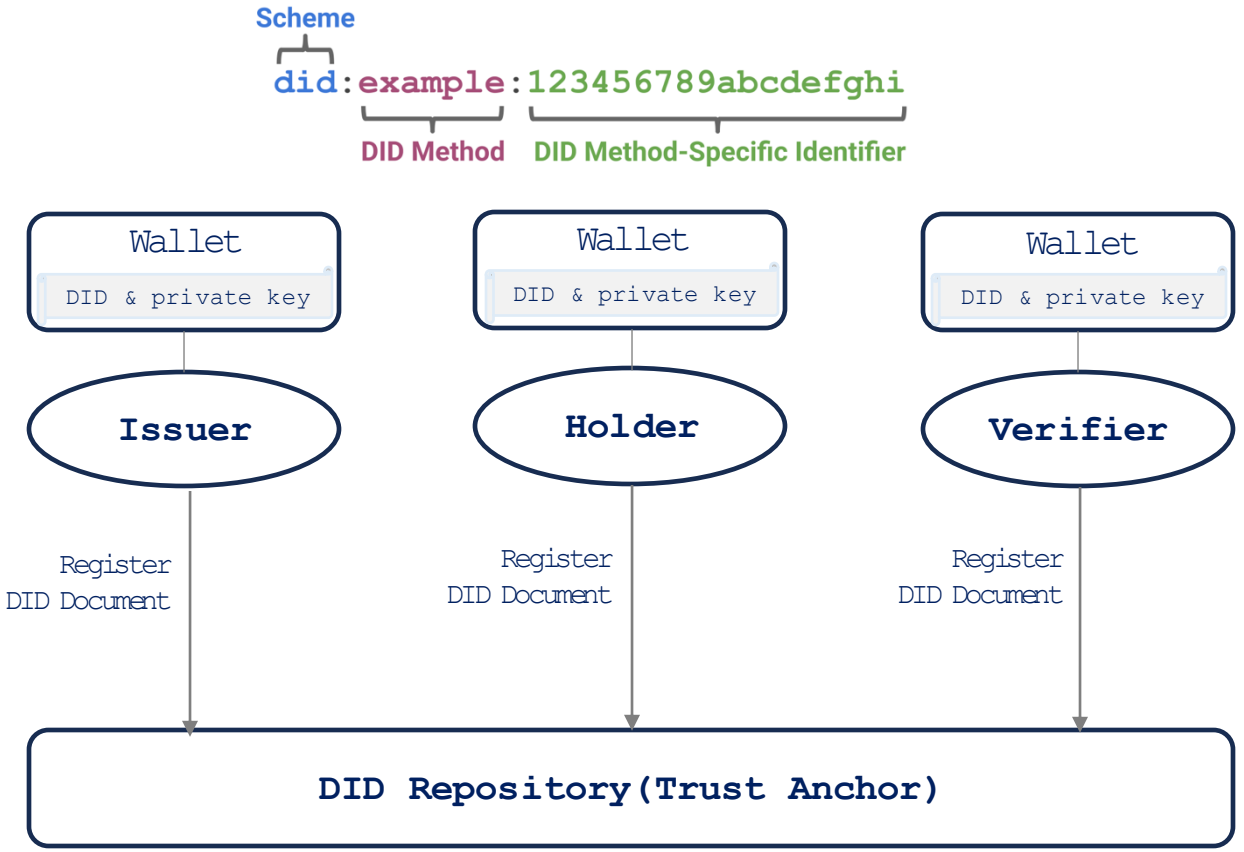
중앙집중형 등록기관이 필요하지 않고, 블록체인과 같이 분산된 네트워크에 등록되는 암호학적으로 검증 가능한 고유식별자

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1"
    "https://w3id.org/security/suites/ws-2020/v1"
 ]
  "id": "did:example:123456789abcdefghi",
  ...
  "verificationMethod": [{
    "id": "did:example:123456789abcdefghi#key-1",
    "type": ...,
    "controller": ...,
    "publicKeyJwk": ...
  }, {
    "id": "did:example:123456789abcdefghi#key-2",
    "type": ...,
    "controller": ...,
    "publicKeyMultibase": ...
  }

  "authentication": {
    "id": "did:example:123456789abcdefghi#key-1"
  },

  "assertionMethod": {
    "id": "did:example:123456789abcdefghi#key-2"
  }
}
```

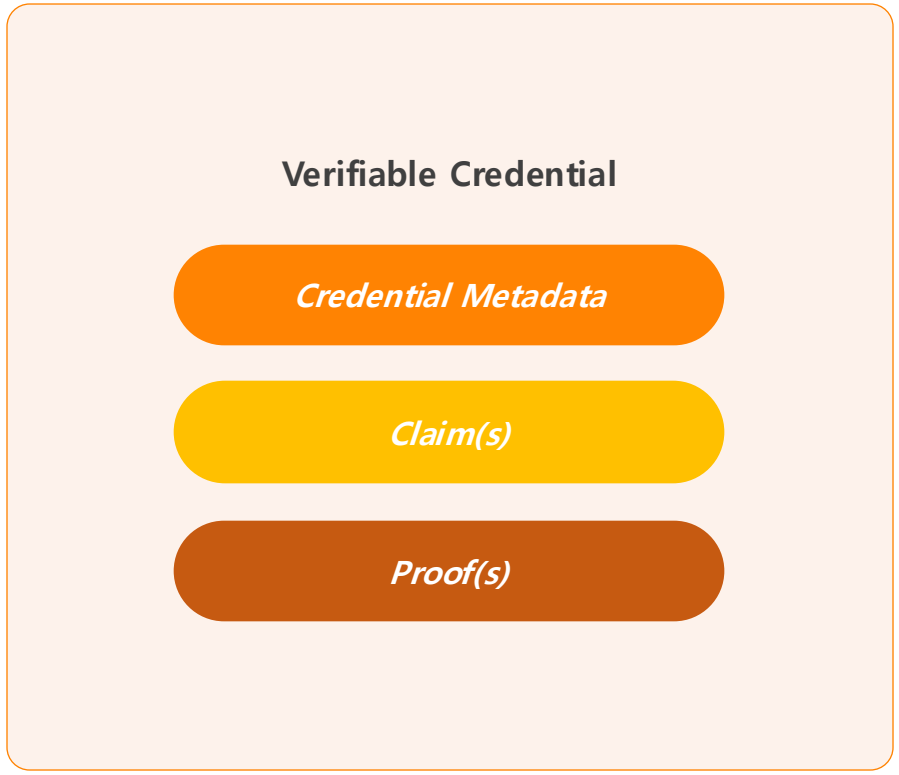
https://www.w3.org/TR/did-core/

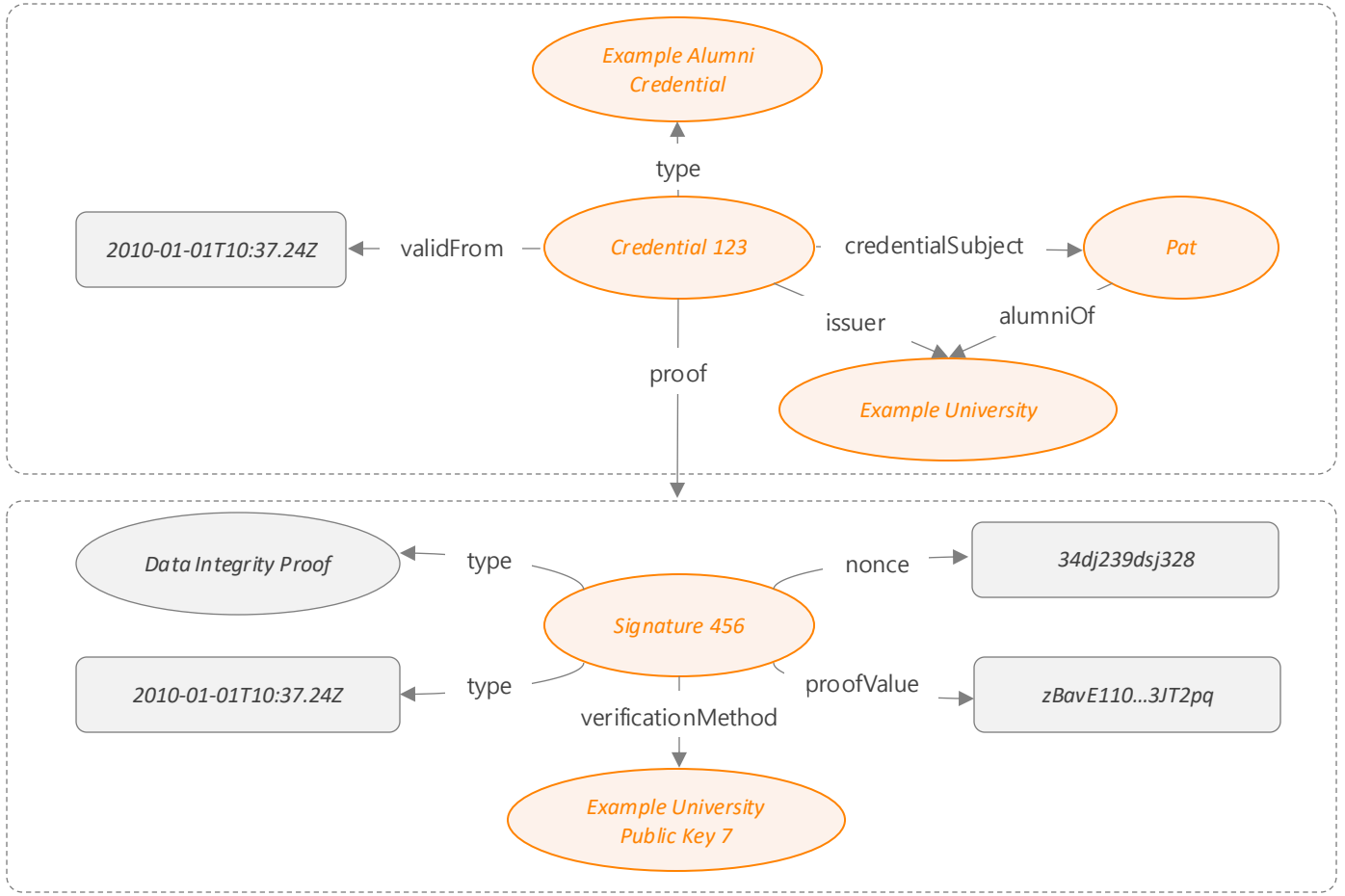


https://www.w3.org/TR/did-spec-registries/

VCs(Verifiable Credentials)는 무엇인가?

A credential is a **set of one or more claims** made by **the same entity.**





https://www.w3.org/TR/vc-data-model-2.0/

03 Open DID Goal and Principle

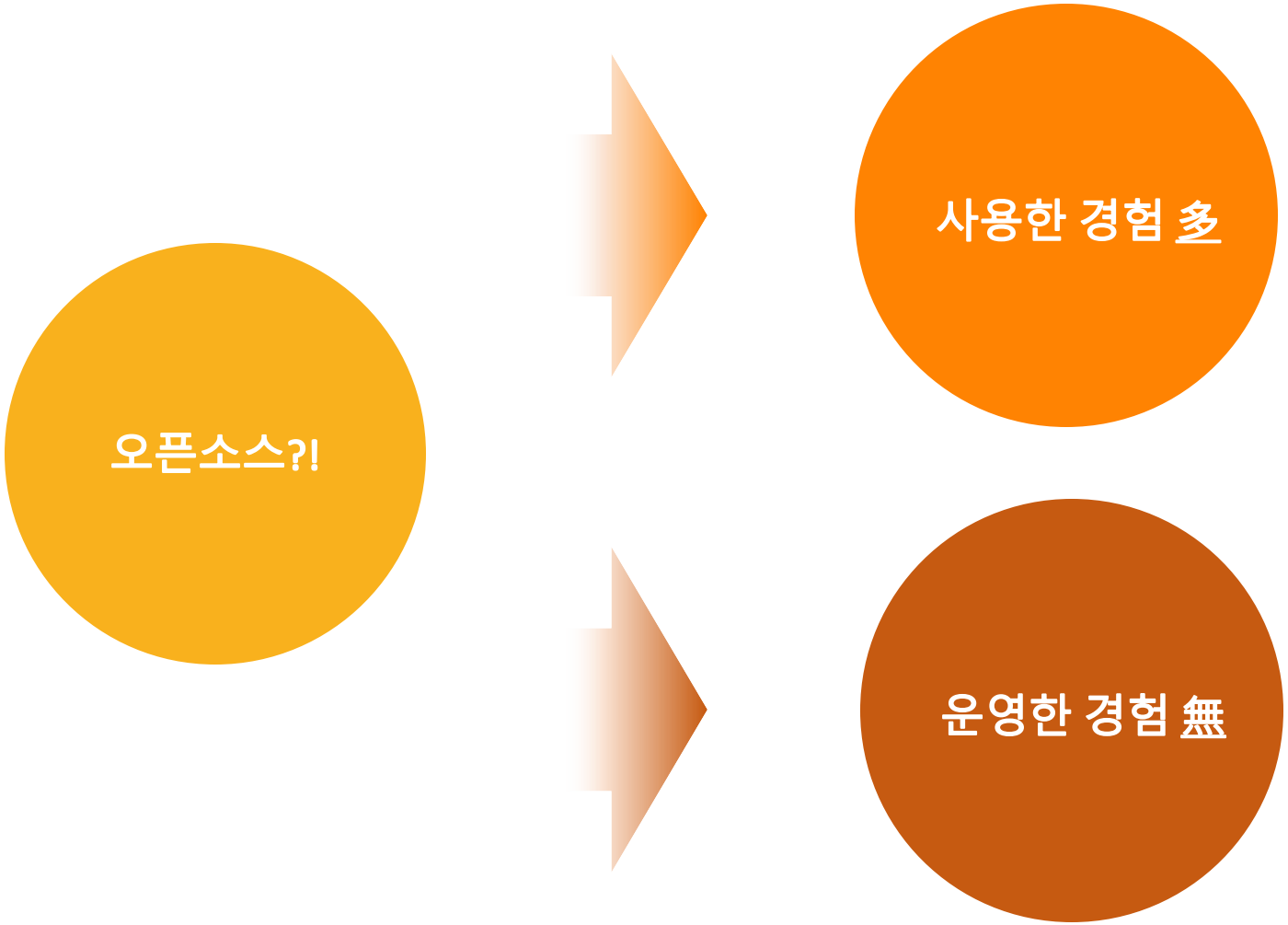
목적

- 한국 디지털정부의 **국가 모바일 신분증 모델을 해외로 확산**
- 전 세계에 디지털 정부 대전환 선도기관으로 국가 브랜드 상승
- Open Source 기반으로 **국제 디지털ID 표준화 선도**
- ESG Perspective 인류 사회 공헌 - 전세계적으로 ID (법적인 신분증명) 을 갖고 있지 않은 사람이 13억 이상 존재 (의료,교육,경제적 혜택 배제). UN SDG 16.9 지속 가능한 개발 Agenda ID4D – 2030까지 모든 인류에게 신분 증명을 제공한다
- World Bank & IDB 등 개도국에 E-Government Initiatives 및 DID 프로젝트 지원 및 기술 기여

원칙

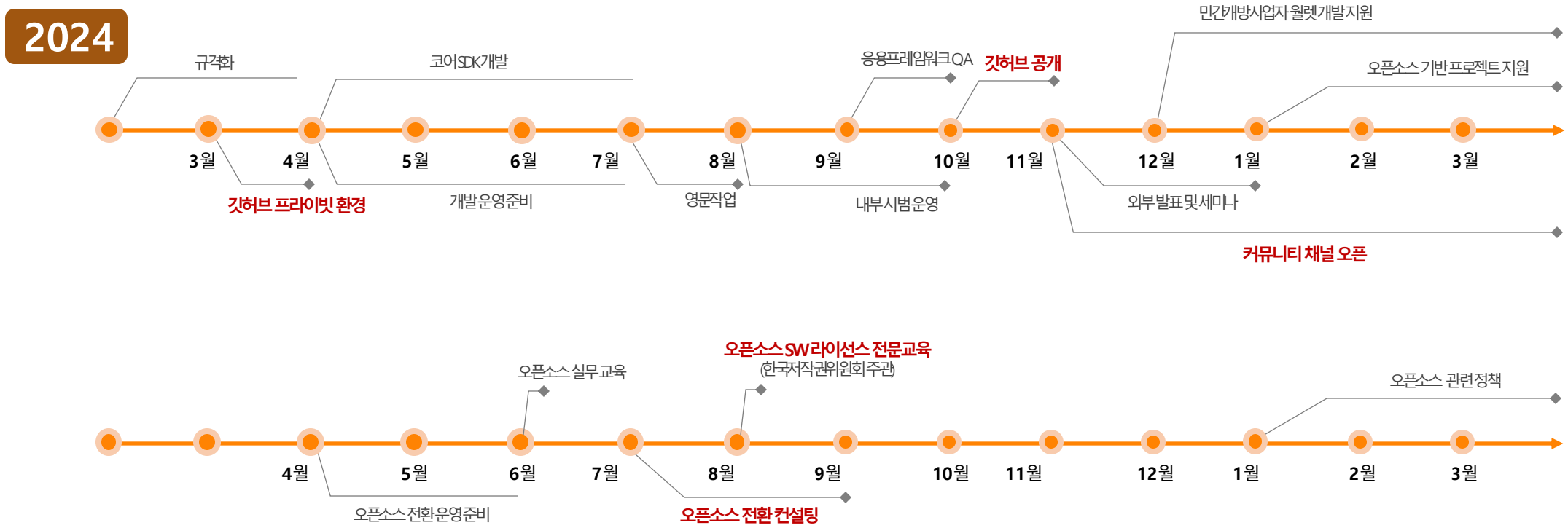
- Trust Framework의 세계화 - Global Trust Framework의 중심, 국가 디지털 신분증 기술을 선도
- 특정 국가, 특정 디바이스에 종속되지 않는 **오픈소스 중심 운영. 확산** - 오픈소스를 통한 K-DID 기술 표준 전파 및 적용 확산, 국가 DID 체계 지원 및 국제간 연계
- 서로 다른 국가 디지털 신분증을 상호 쉽게 검증할 수 있도록 국제표준화 진행 - ISO, ITU, W3C, TTA등 국제 표준화 연구 및 적용을 통한 K-DID 글로벌 확산

04 Open DID 진행 과정



04 Open DID 진행 과정

진행 과정



05 오픈소스 주요 컨설팅 내용

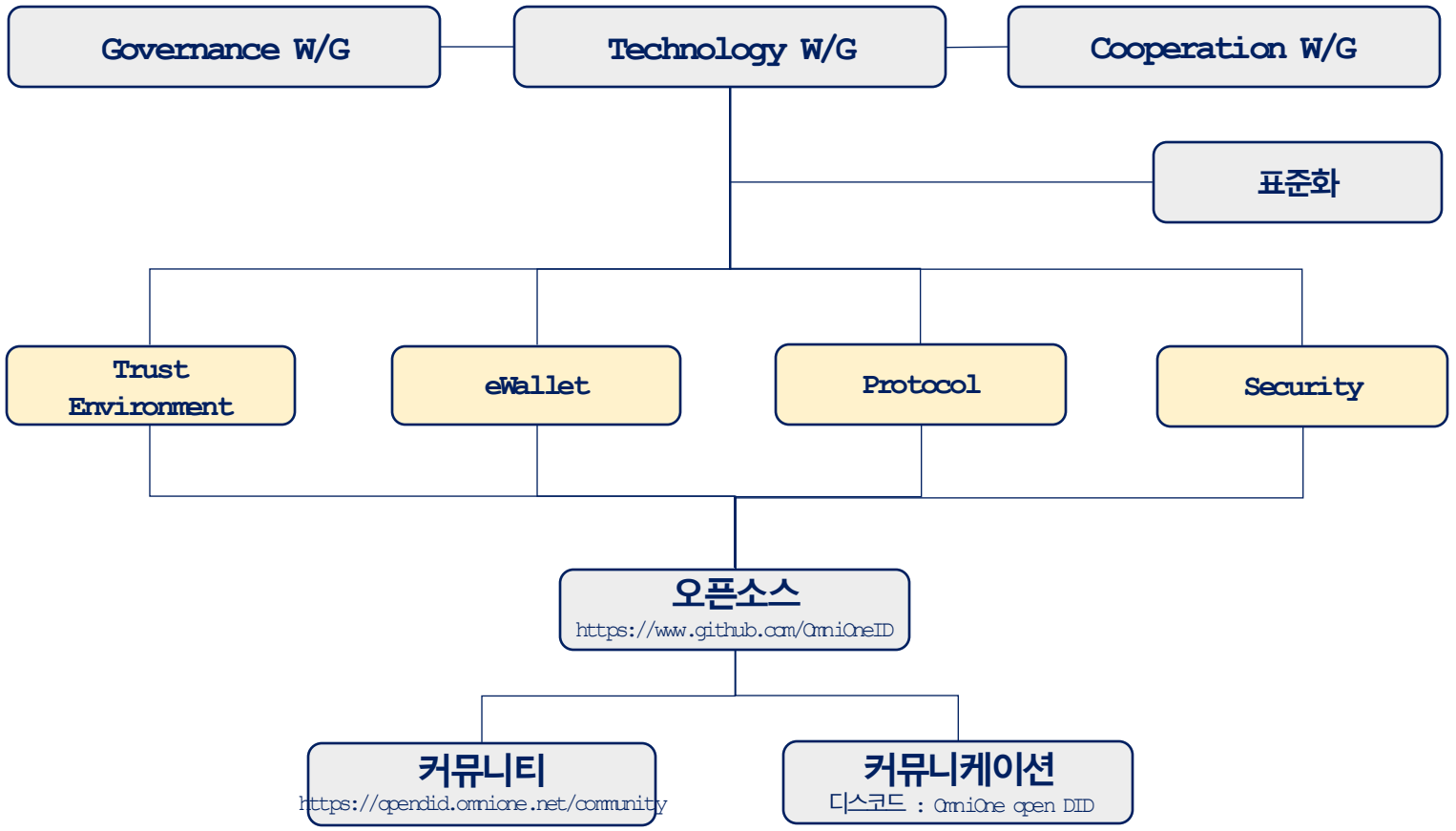
오픈소스 비즈니스 모델 수립	거버넌스 체계 구축	라이선스 및 공급망 관리	커뮤니티 구축 및 운영 전략	품질 관리 및 성과 지표 관리
DID 기술의 오픈소스화를 통한 비즈니스 기회 창출 방안 수립	오픈소스 커뮤니티 관리 및 운영을 위한 거버넌스 체계	오픈소스 전환에 따른 라이선스 이슈 해결	오픈소스 커뮤니티 활성화 방안 수립	지속적인 품질 관리를 위한 CI/CD 도입 및 운영 방안
지속 가능한 수익 모델 제안	책임과 권한 분배 및 운영 방안 마련	소프트웨어 공급망에 대한 관리 방안 제안 (SBOM 관리 포함)	기여자 관리 및 커뮤니티 성장 계획 제안	성과 지표 정의 및 개선 방안 마련

* 공개 SW R&D 실무 수행 가이드라인(과학기술정보통신부, 2022) 에 기반하여 컨설팅

* 오픈소스 R&D 역량 성숙도는 한국정보통신기술협회의 단체표준인 "공개소프트웨어 기반 개방형 혁신 연구개발 역량 성숙도 모델" 을 기반으로 관리

06 오픈소스 워킹 그룹

워킹 그룹 및 개발 구성



오픈소스 활동

❑ Trust Enviroment

- 참가 엔티티 신뢰보장 환경 구성에 대한 연구
- 신뢰등록/해지에 대한 표준 소스 개발

❑ eWallet

- 상호호환용 범용월렛에 대한 연구
- VC 데이터포맷 기반 표준 소스 개발
- mDoc / XML 등 다양한 포맷 수용 예정

❑ Protocol

- 발급 / 제출 프로토콜에 대한 연구
- 온라인(Rest API) 기반 표준 프로토콜 개발
- 온라인 확장(OID4XX), 오프라인(NFC/BLE) 표준 메시지규격 확장 예정

❑ Security

- 프라이버시보호, 안전한 통신 등에 대한 연구
- 키 보호 방안에 대한 표준 소스 개발
- ZKP, 선택적 제출, 통한 프라이버시 보호 예정

❑ 커뮤니티/커뮤니케이션

- 컨트리뷰터와의 커뮤니케이션
- 활동 내용에 대한 공개

07 Open DID 대상 및 개발

오픈소스 대상

- 신뢰시스템, 체인코드, 이슈어시스템, 검증시스템, 월렛에 적용된 주요 컴포넌트
- 데모용 신뢰서버, 데모용 이슈어서버, 데모용 검증서버, 데모용 월렛

개발 기본 원칙

기술 독립성
- 특정 기술이나 도구 의존성을 최소화하고 다양한 기술을 포용 및 호환할 수 있도록 설계한다

독립적 동작
- 구성 요소간 의존성을 최소화하여, 개별적으로 동작할 수 있어야 한다.

문서화
- 지속가능한 관리 및 기술 선택을 위해 설계, 구현, 운영에 대한 문서를 제공한다

표준 준수
- 기술 구현 시 개방형 표준(Open standards, preventing vendor and technology lock-in)을 준수한다

자유로운 기여
- OPEN DID 프로젝트에 누구라도 자유롭게 기여할 수 있다

투명성
- 프로젝트의 결정 및 변경 사항에 대해서는 투명하게 공개한다

상업용 라이선스 제한
- OPEN DID의 모든 컴포넌트 내에서는 상업용 라이선스 사용을 금지한다

원칙 준수
- 각 원칙은 다른 원칙을 위반하지 않는 선에서 시스템 설계와 구현에 적용되어야 한다

07 Open DID 대상 및 개발

08 Open DID 라이선스

	복제, 배포, 수정의 권한허용	배포시 라이선스 사본첨부	저작권 고지사항 또는 Attribution 고지사항 유지	배포시 소스코드 제공의무와 범위	조합저작물 작성 및 타 라이선스 배포허용	수정내용 고지	명시적 특허 라이선스의 허용	라이선시가 특허소송 제기시 라이선스 종료	이름, 상표, 상호에 대한 사용제한	보증의 부인	책임의 제한
MIT License	O	O	O		조건부					O	O
Apache License 2.0	O	O	O		O		O	O	O	O	O
BSD(Berkeley Software Distribution)	O	O	O		조건부				O	O	O
GPL(General Public License) 3.0	O	O	O	전체 코드		O	O	O		O	O
LGPL(Less GPL) 3.0	O	O	O	2차 저작물	O	O	O	O		O	O
MPL(Mozilla Public License) 1.1	O	O	O	파일 단위	O	O	O	O		O	O

09 Open DID 구조

공개 내용

Document

1. did-doc-architecture
2. did-release

Mobile Application

1. did-ca-aos
2. did-ca-ios

Mobile SDK

1. did-client-sdk-aos
2. did-client-sdk-ios

Server Application

1. did-fabric-contact
2. did-issuer-server
3. did-ta-server
4. did-verifier-server
5. did-api-server
6. did-ca-server
7. did-demo-server
8. did-wallet-server

Server SDK

1. did-blockchain-sdk-server
2. did-core-sdk-server
3. did-crypto-sdk-server
4. did-datamodel-sdk-server
5. did-wallet-sdk-server
6. did-cli-tool-server
7. did-common-sdk-server

소스 :
https://github.com/OmniOneID

커뮤니티 :
https://opendid.omnione.net/community/

문서 :
https://omnioneid.github.io/?locale=en&version=V1.0.0#/

주요 내용 설명

did-fabric-contract	패브릭용 스마트컨트랙트	**did-ca-server**	월렛 인터랙션용 사용자 가입 서버	**did-blockchain-sdk**	블록체인인터랙션용 SDK
did-ta-server	신뢰에이전트용 서버	**did-ca-ios**	iOS 월렛 인터랙션용 사용자 앱	**did-api-server**	블록체인 접근용 공개 API 서버
did-issuer-server	발급기관용 서버	**did-ca-aos**	Android 월렛인터랙션용 사용자 앱	**did-demo-server**	VC 발급/제출용 데모 서버
did-verifier-server	검증기관용 서버	**did-client-sdk**	월렛용 SDK	**did-demo-app**	VC 발급/제출용 데모 앱

10 25년 활동계획

❑ 오픈소스 개발

✓ 신뢰환경 구성 플러그인 확장
- BESU용 컨트랙트 확장 대응
- 엔티티 라이프사이클 관리

✓ 범용 월렛 구현
- 월렛 호환 아키텍처
- mDoc data model 지원
- Kotlin 언어 지원

✓ 프로토콜 확장
- 발급 프로토콜 확장(OID4VC)
- 제출 프로토콜 확장(OID4VP)

✓ 프라이버시 보호 강화
- zk-snark 프로토콜 기반 영지식증명
- 키/메시지 보호 알고리즘 강화

❑ 표준 활동

✓ ITU-T
- 신뢰가능한 디지털월렛 라이프사이클 관리
- 다양한 데이터포맷 관리
- 선택적 제출 위한 BBS+ Signature 연구

✓ ISO/IEC
- 영지식증명(zkp)표준 공헌
- 선택적 제출(SD-JWT)표준 공헌

✓ TTA
- 분산식별자 기반 모바일신분증 신규 표준 개정

✓ FIDO Alliance
- FDO & DID 결합 방안 제안

10 25년 활동계획

❑ 오픈소스 확대 지원

✓ 행안부 월렛 표준 관리
- 모바일신분증 월렛 기술 규격 관리
- 민간사업자 협력 통한 월렛 개선 관리

✓ 해외 디지털아이디 오픈소스 적용 지원
- 인니 Digital ID에의 오픈소스 가이드
- 코타 워킹그룹 오픈소스 가이드

✓ 해커톤 지원
- 오픈소스 활용에 대한 기술 멘토링
- BESU 플랫폼 활용에 대한 가이드

❑ 워킹그룹 활성화

✓ 컨트리뷰터 활동
- 정기 온오프 연구반 운영(격월 운영)
- 활동 결과에 대한 커뮤니티사이트 게시
- 대학로드쇼/세미나 등 홍보활동 적극 지원
- 모바일신분증 민간사업자와의 정기 회의 통한 기술분과 활성화 및 위상 제고

✓ 서브그룹 운영
- 4개 서브그룹 본격 운영(7월)
- 타 표준단체와의 교류 활성화(DIF/OIDC 등)

❑ 오픈소스 개발

✓ 오픈소스 이용 편의성 강화
- Downloadble sample module 구성
- Sample demo page 구성

Q & A

Thank You

Contact Us

contact@raoncorp.com

www.raoncorp.com