블록체인 기반 자기주권형 모바일 전자증명 서비스

2019. 8. 29

SK텔레콤 블록체인 인증 Unit 송지영

과학기술정보통신부 KISA

SK telecom 컨소시엄

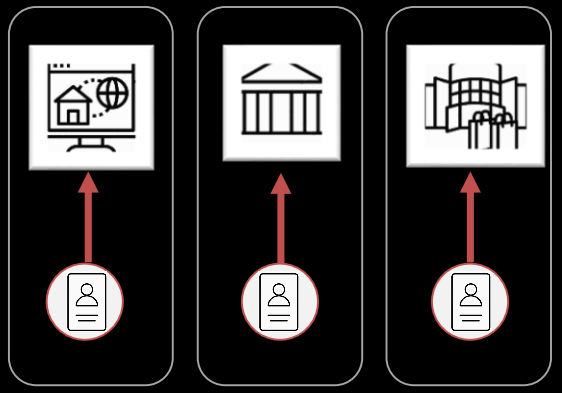
왜 '프라이버시(Privacy)' 위기인가?

디지털화가 가속화될수록 개인정보 침해와 유출사고 빈번해짐에 따라 전세계적으로 개인정보 보호의 중요성에 대한 인식이 확산되고 있음

- ✓ (글로벌) 국내외 빈번한 개인정보 유출사고의 발생에 따른 개인정보 보호에 대한 관심과 대응책 준비 노력 확대
- ✓ (글로벌) 블록체인 기술의 등장과 개인정보관리의 중앙집중화에 반대하는 분산신원 관리 모델 부상
- ✓ (국내) 번거로운 공인인증서의 폐지 관련한 법/제도 개정 논의의 시작

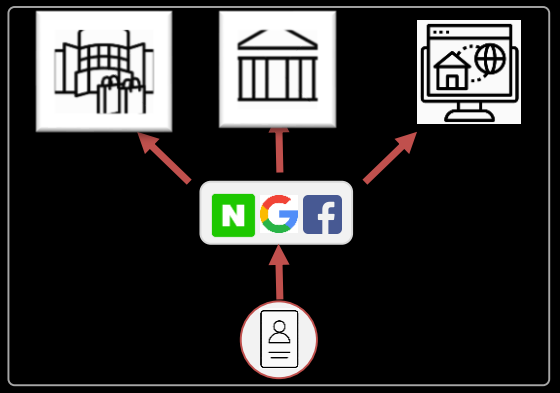
‘신원(Identity)’ 모델의 진화

개별 신원 모델 (Siloed Identities)



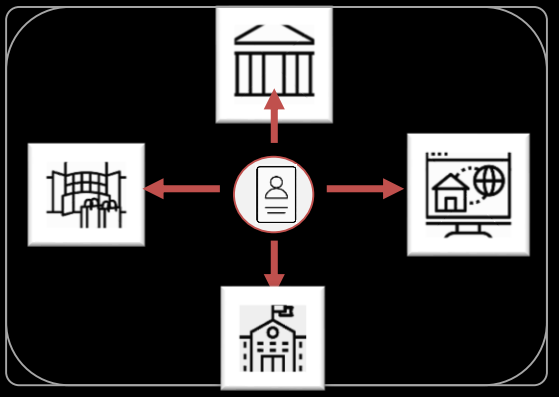
- ▪형태
  - 여러 인터넷 사이트에서 각각 ID/PW 발급 받아 사용
- ▪특징
  - 수많은 인터넷 사이트에 서로 다른 ID/PW로 가입 후 ID/PW 분실 시 번거로움 존재
  - 단일한 ID/PW 사용 시 위험증가

연합 신원 모델 (Federated Identities)



- ▪형태
  - OpenID, OAuth 등을 기반으로 기존 소셜 미디어 계정으로 다른 앱, 사이트에 로그인
- ▪특징
  - 특정 서비스에 개인 정보가 집중됨에 따라 개인 정보 유출 시 상당한 위험 존재

자기주권 신원 모델 (Self-Sovereign Identities)

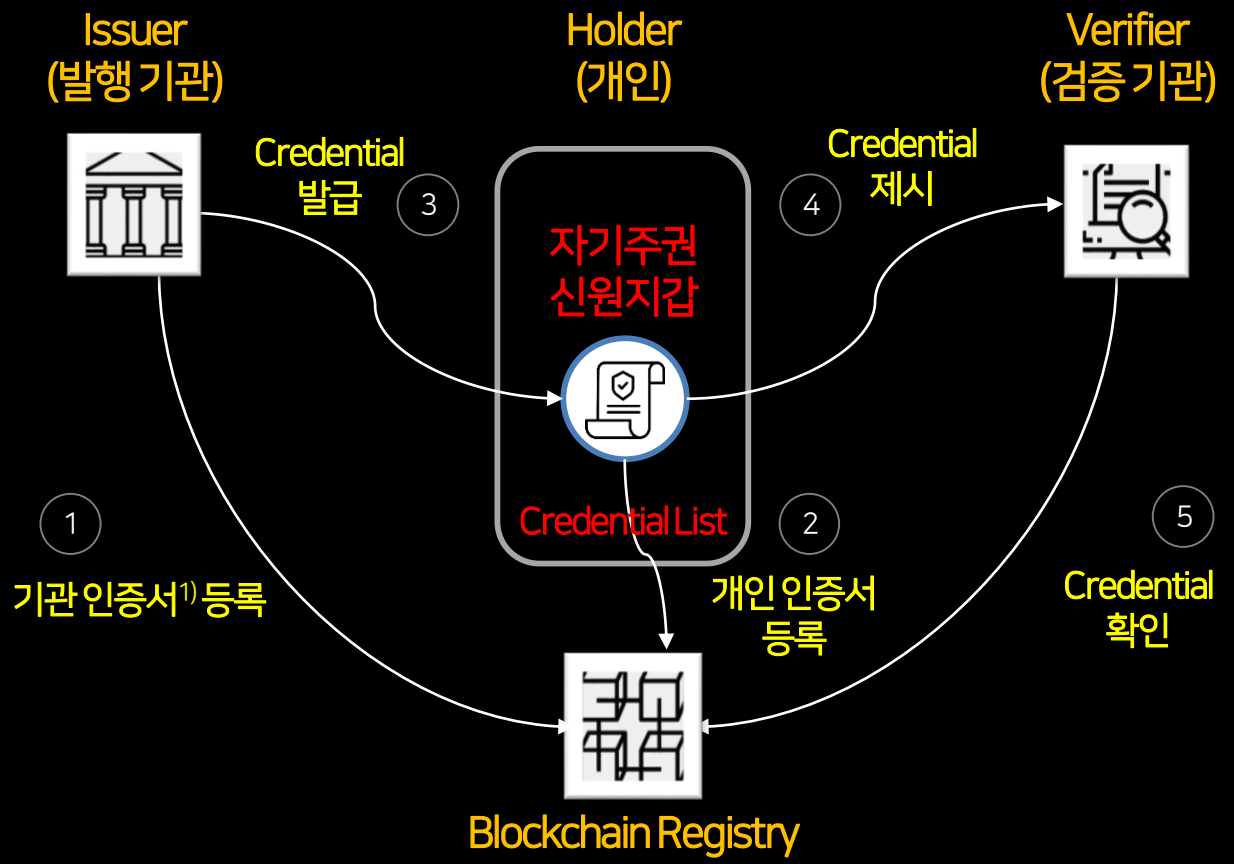


- ▪형태
  - 모바일 단말로 신원 증명 제출을 통한 다양한 서비스 이용
- ▪특징
  - 개인정보를 본인이 직접 단말(앱 클라이언트) 내에 관리
  - 단말 분실 시 위험 존재

분산 신원(DID; Decentralized Identifier)의 출현

SSI 구현과 확산을 위해 국제 웹 표준기구인 W3C 주도로 분산 신원(DID; Decentralized Identifiers) 모델에 대한 표준화가 진행 중

개념도



Note: 1) 기관 인증서는 해당 기관의 DID 값, public key, 서비스 접근 주소로 구성됨

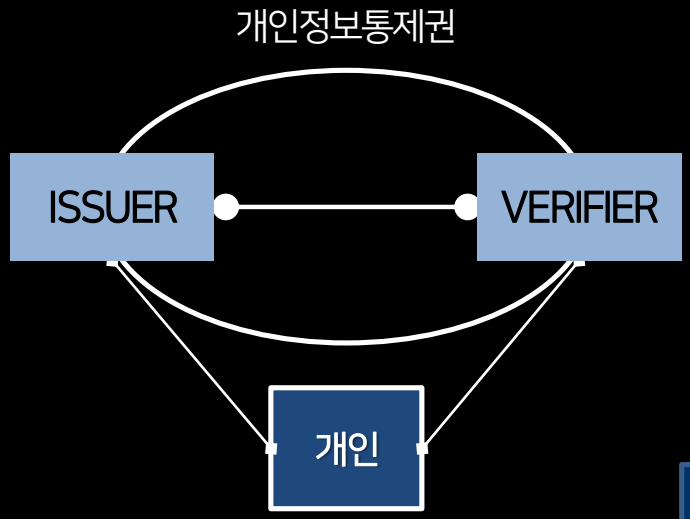
특징

- 블록체인을 PKI(공개키 인프라; public key infrastructure)로 사용
- Credential(자격증명 데이터) 사용자 기기에 저장
- Verifier가 개인정보 저장하지 않고 고객이 제공한 정보만 검증

'자기주권 신원(SSI; Self-Sovereign Identity)'이란?

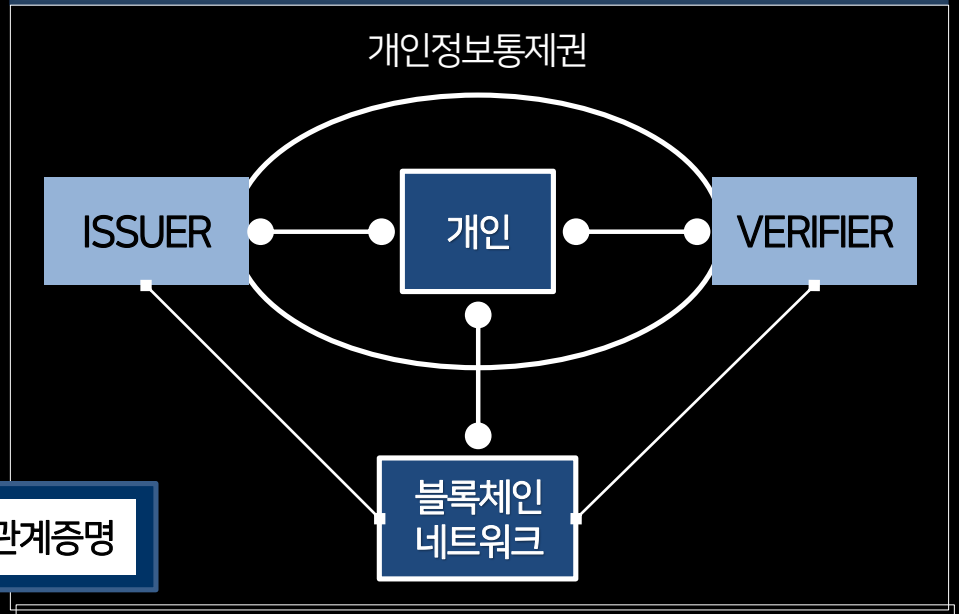
자기주권 신원 모델이란 기업이 개인정보를 통제하는 방식이 아닌, 개인이 직접 개인정보와 관련된 증명 발급과 제출을 수행하는 방식

(AS-IS) 중앙집중형 / 연합형 신원 모델



Verifier가 개인에게 개인 정보(로그인 등)를 요청할 경우 Issuer가 (개인의 동의 하에) 제공해주는 방식

(TO-BE) 자기주권형 신원 모델



개인은 Issuer에게 개인 정보 관련 증명 발급을 요청하고, 발급받은 증명을 Verifier에게 전달하는 방식

자기주권 신원(SSI; Self-Sovereign Identity) 요건

자기주권 신원 모델이란 신원 주체 본인 이외의 기관에 의존하지 않고, 장기적 소유와 이동이 가능한 안전한 신원관리를 지향함.

SSI 10대 원칙 *by Christopher Allen*

1. Existence – 사용자는 독립적 존재이어야 한다
2. **Control** – 사용자는 그들의 **신원정보에 대한 통제권**을 가져야 한다
3. Access – 사용자는 그들의 신원데이터에 접근 가능해야 한다
4. **Transparency** – **시스템과 알고리즘**은 **투명**해야 한다
5. **Persistence** – 신원정보는 **장기간** 저장되어야 한다
6. **Portability** – 신원정보와 서비스는 **이동 가능**해야 한다
7. **Interoperability** – 신원정보는 가능한 **널리 사용**되어야 한다
8. **Consent** – 사용자는 그들의 신원정보 사용에 대해 **동의**하여야 한다
9. Minimize – Claim 의 사용은 최소화 되어야 한다
10. **Protection** – 사용자의 **권리는 보호**되어야 한다

<Source : http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>

자기주권형 '분산 신원(DID)' 모델로 무엇을 할 것인가?

"디지털 자기주권을 기반으로 중개자 없이 개인의 신원을 증명하자!

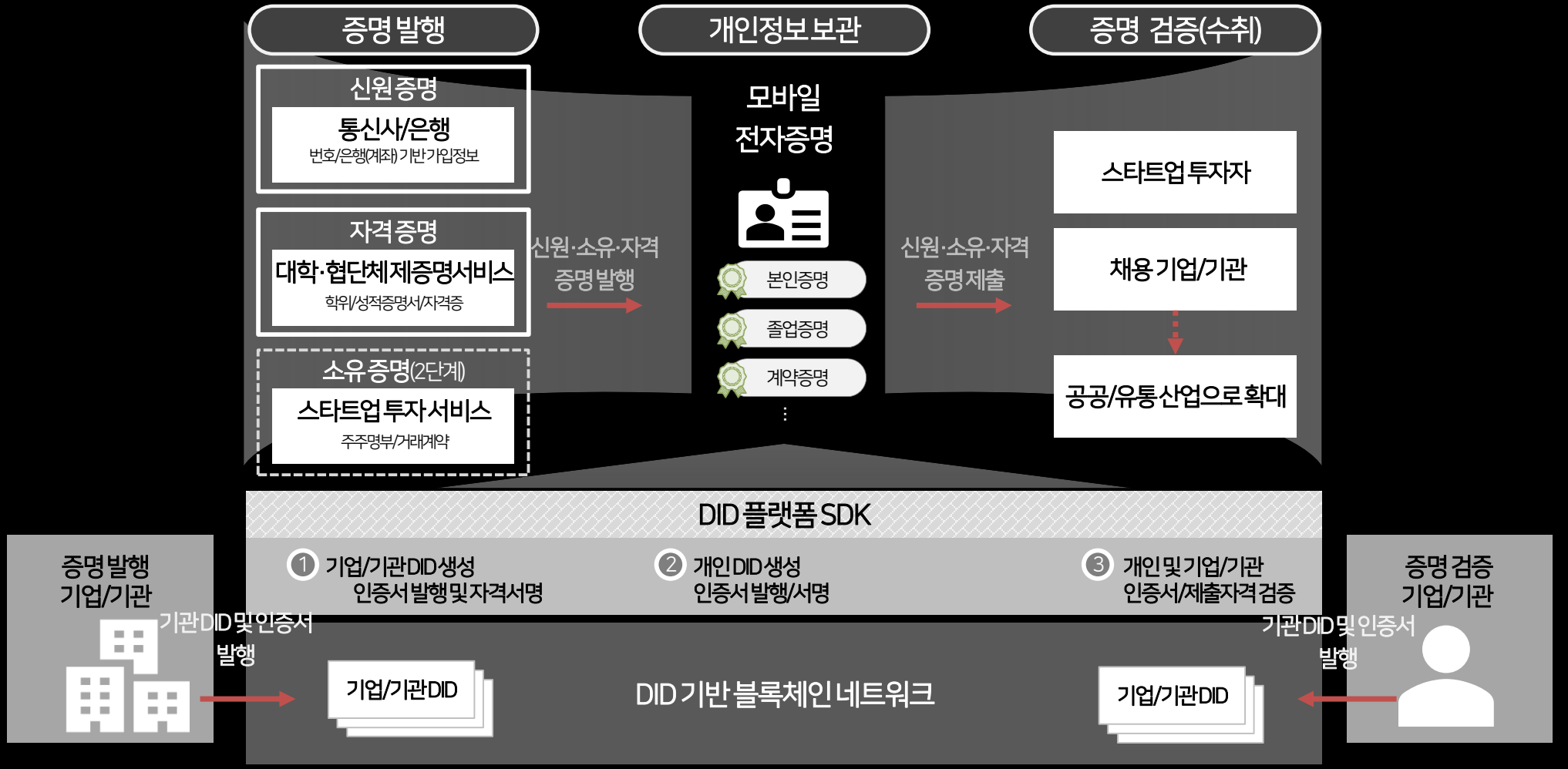
나의 개인정보를 내 **단말에 저장하고, 필요 시 직접 제출**할 수 있는 서비스

신뢰 기반의 증명서 발행과 증명서 검증이 가능한 **DID**(Decentralized ID) **블록체인 인프라**

증명 발행과 증명 확인 기관 간의 직접적인 연결을 제거함으로써 개인의 프라이버시 보호

블록체인 기반 자기주권형 모바일 전자증명 서비스

자기주권형 모바일 전자증명 서비스는 블록체인 네트워크와 플랫폼 SDK를 이용해 DID(Decentralized Identifier) 기반의 증명서 발행 및 제출/검증을 위한 플랫폼 제공



모바일 전자증명 서비스 주요 기능

모바일 전자증명 어플리케이션은 각종 증명서를 단말에 발급 받아 저장하고 기관에 제출하는 기능 및 전자계약을 위한 전자서명 기능으로 구성

1. 전자증명서

발급 완료한 증명서의 자세한 내용 및 상태를 조회하고 관리 가능

2. 증명서선택

필요한 증명서를 선택하여 발급 신청하는 기능

3. 발행기관선택

기관을 선택하여 발급이 가능한 증명서를 신청하는 기능

4. QR 스캔

QR스캔 기능으로 기관과 연결하여 증명서를 발급/제출 하는 기능

5. 전자계약서

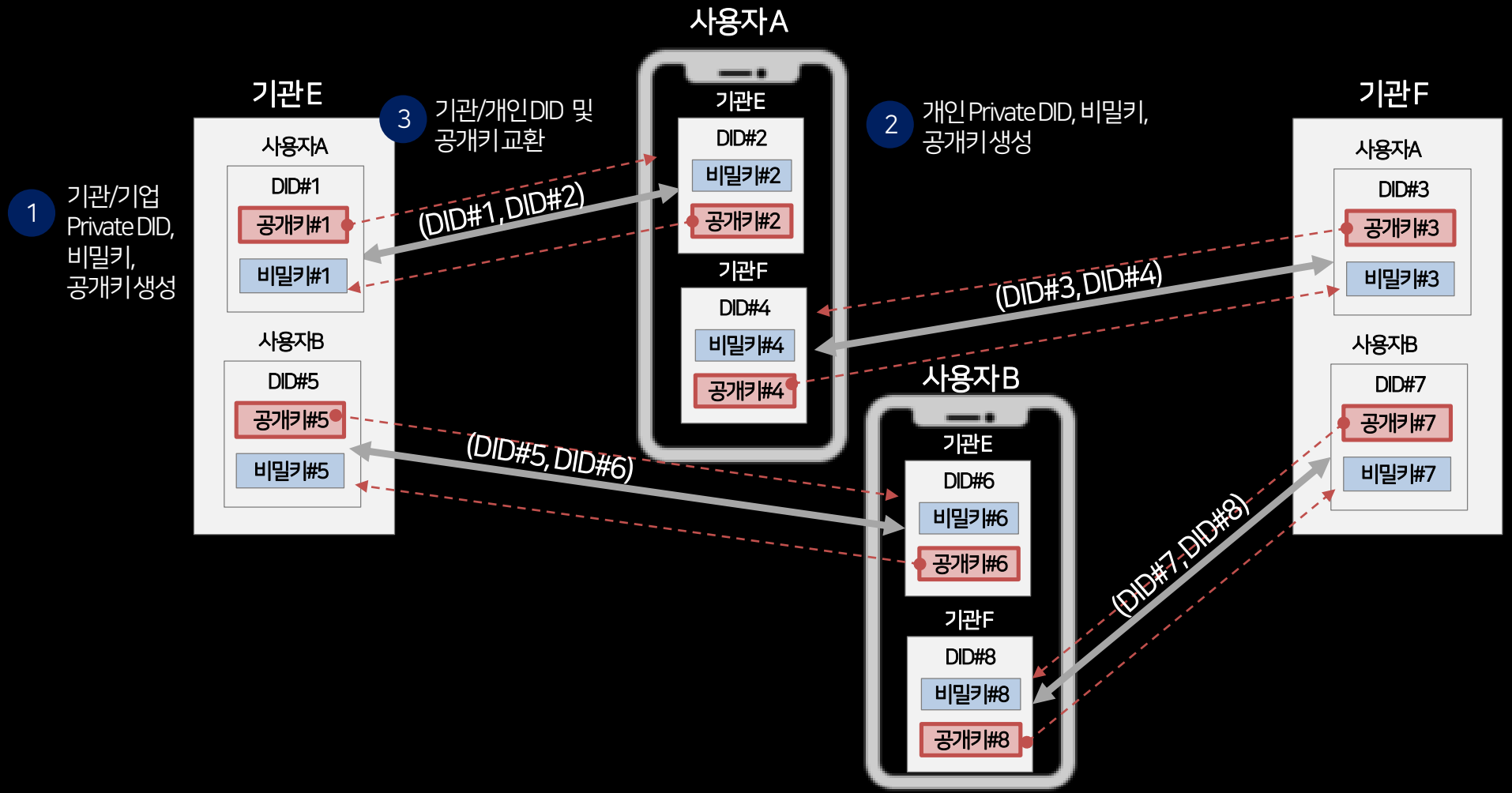
전자계약서를 DID로 서명 후 모바일 내에서 관리 기능

6. 리워드쿠폰

행위에 따라서 OTX로 교환 가능한 리워드 발행 기능

주요 특징 : 사용자와 발급기관/수취기관 간 독립적 연결 구조

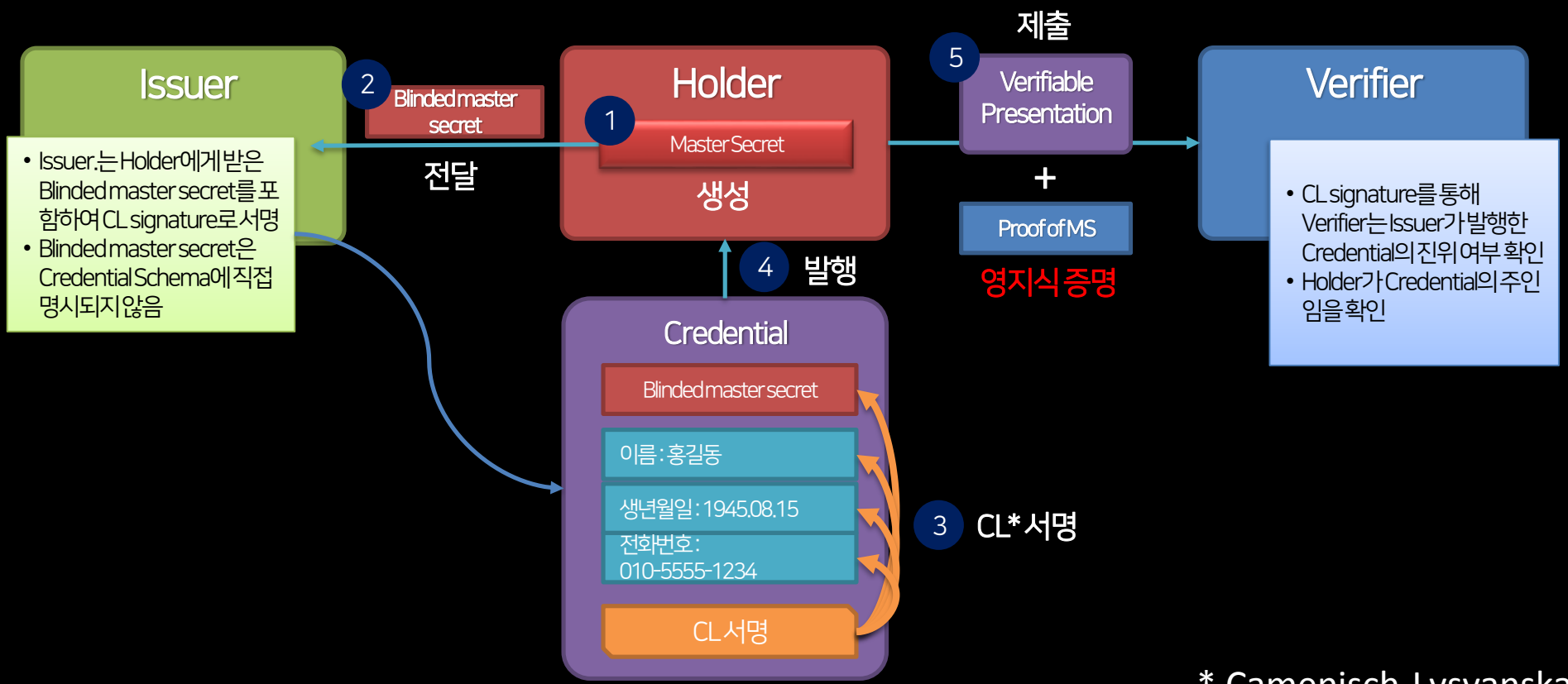
기관-개인 간 상호 독립적인 Pairwise-DID 방식의 연동을 통해 각 기관에 저장된 개인정보에 대한 연결 정보(CI)를 제거함으로써 프라이버시 보호



주요 특징 : 영지식 증명 기반 증명서(Credential) 발행 및 검증

영지식 증명을 통해 사용자의 익명성을 보장하면서 증명서의 소유자임을 증명

- 소유권 증명을 위해 증명서 내에 주인(Subject)를 직접 명시함으로써 발생할 수 있는 프라이버시 및 보안 문제 해결
- 발행자(Issuer)는 사용자(Holder)만 알고 있는 마스터 비밀 값(master secret)을 반영하여 증명서 발행
- 증명서 제출시 본인의 마스터 비밀 값(master secret) 노출 없이 영지식 증명을 통해 소유권 증명

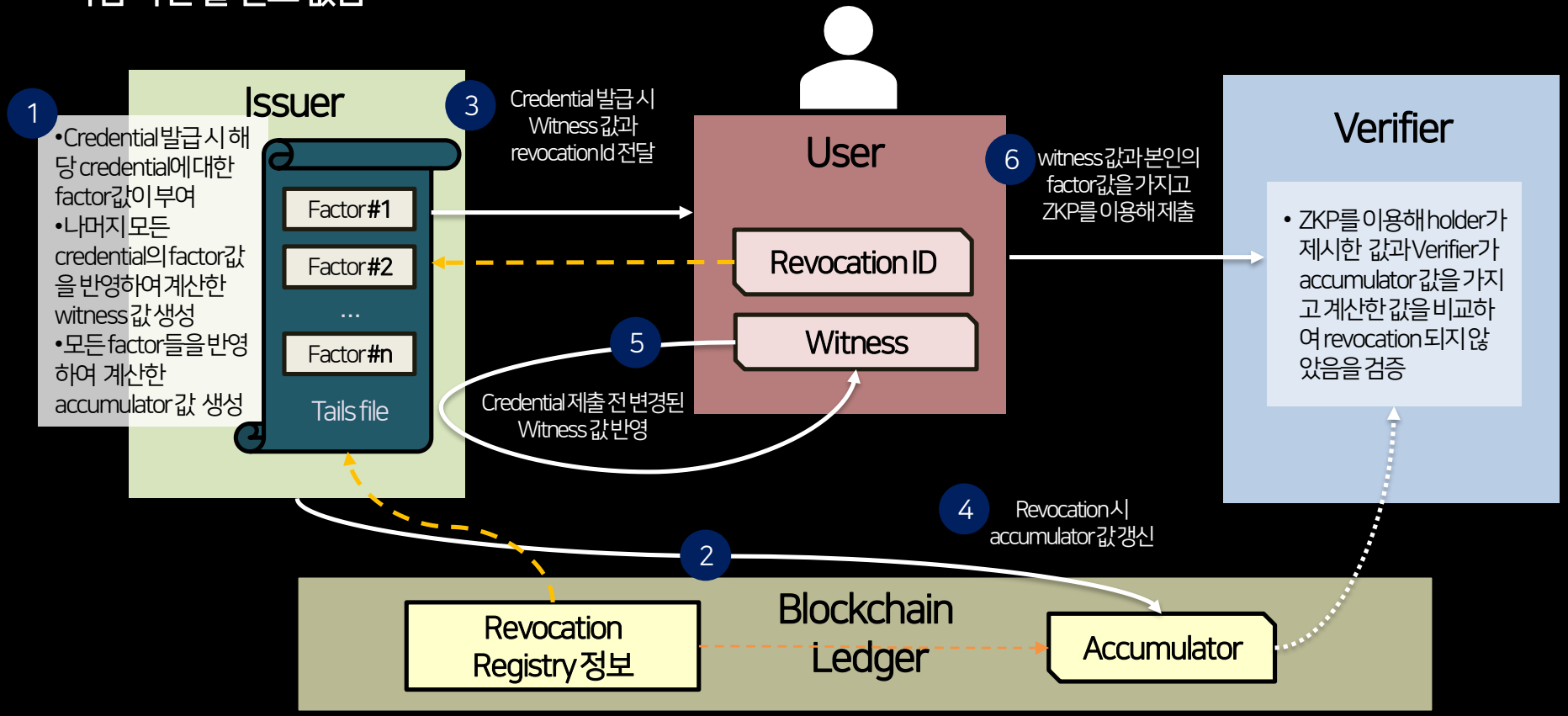


* Camenisch-Lysyanskaya

주요 특징 : 발행된 증명서의 안전한 폐기(Revocation)

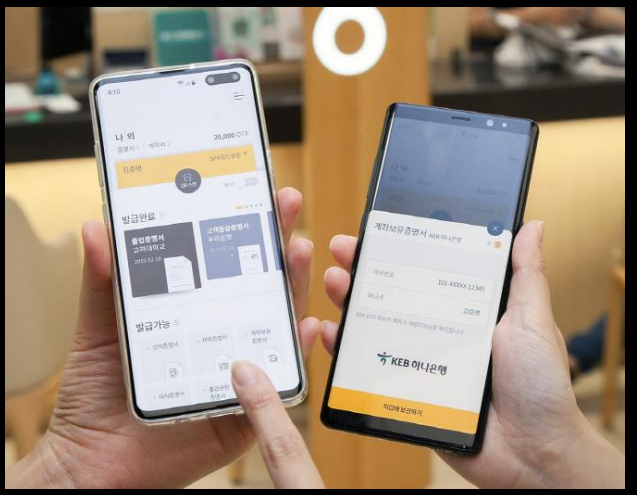
개인정보를 보호 하는 방식으로 증명서 폐기 여부 확인 및 검증

- 각 증명서에 부여된 고유 값을 바탕으로 계산되는 암호적 누적 값(cryptographic accumulator)를 원장(ledger)에 공유하여 폐기(revocation) 여부 검증
- 발행된 증명서의 폐기를 위해 발행자가 사용자 또는 검증자에게 요청하거나, 폐기 여부 확인을 위해 검증자가 발행자에 직접 확인 할 필요 없음



사업화 파트너십 추진

- ✓ **컨소시엄 내 노드 참여 5개사와 삼성전자와 KT를 포함한 7개사 사업협약 체결(7.12)**
  - SK텔레콤, LGU+, KT, 삼성전자, KEB하나은행, 우리은행, 코스콤
- ✓ **모바일 전자증명 기반 대학제증명 서비스 관련 1차 공개설명회 개최(8.27)**
  - 전국 30여개 대학 교무처/정보통신처 및 정부기관 관계자 참석
- ✓ **공공문서 전자증명서 연계를 위한 행정안전부 전자증명서사업단 협력 추진**
  - 주민등록등·초본 포함 13종 증명서 제출을 위한 시스템 연계 예정(~'19.12월)



향후 계획

다양한 분야에서 자격, 자산 소유 및 행위 증명으로 영역을 확대하고 자기주권형 데이터 BM 창출