IT R&D Global Leader

블록체인 프라이버시를 위한 영지식증명 기술

ETRI 한국전자통신연구원
www.etri.re.kr
지능화융합연구소/정보보호연구본부

목 차

1. 기술의 개요

▣ 목적

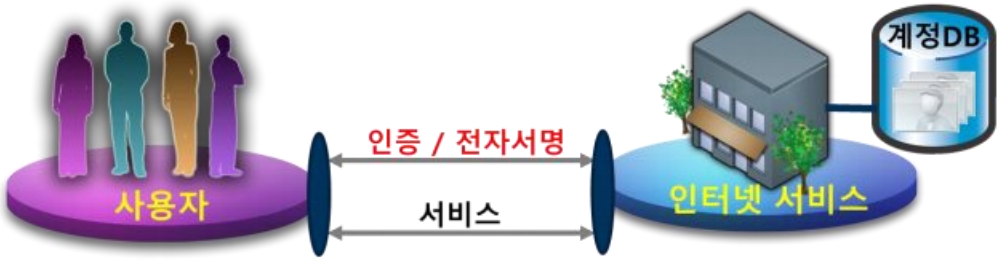
- ❖ 블록체인 기반의 분산ID 기술에서 디지털 신원자격 증명 시, 사용자가 검증자(서비스제공자)에게 개인정보를 선택적으로 노출하여도, 노출하지 않은 개인정보의 유효성(또는 적합성) 여부를 확인할 수 있는 기술

▣ 특징

- ❖ 검증가능한 신원자격 (Verifiable Credential, VC)의 “CredentialSubject” 내, 전체 또는 사용자에 의해 선택된 일부 속성에 대한 은닉 서명 제공
- ❖ 국제 표준을 준용한 검증가능한 프리젠테이션 (Verifiable Presentation, VP) 생성 및 검증

2. 기술의 배경

▣ 현재 신원관리 기술 예시



안전 → 편리

인터넷 초창기

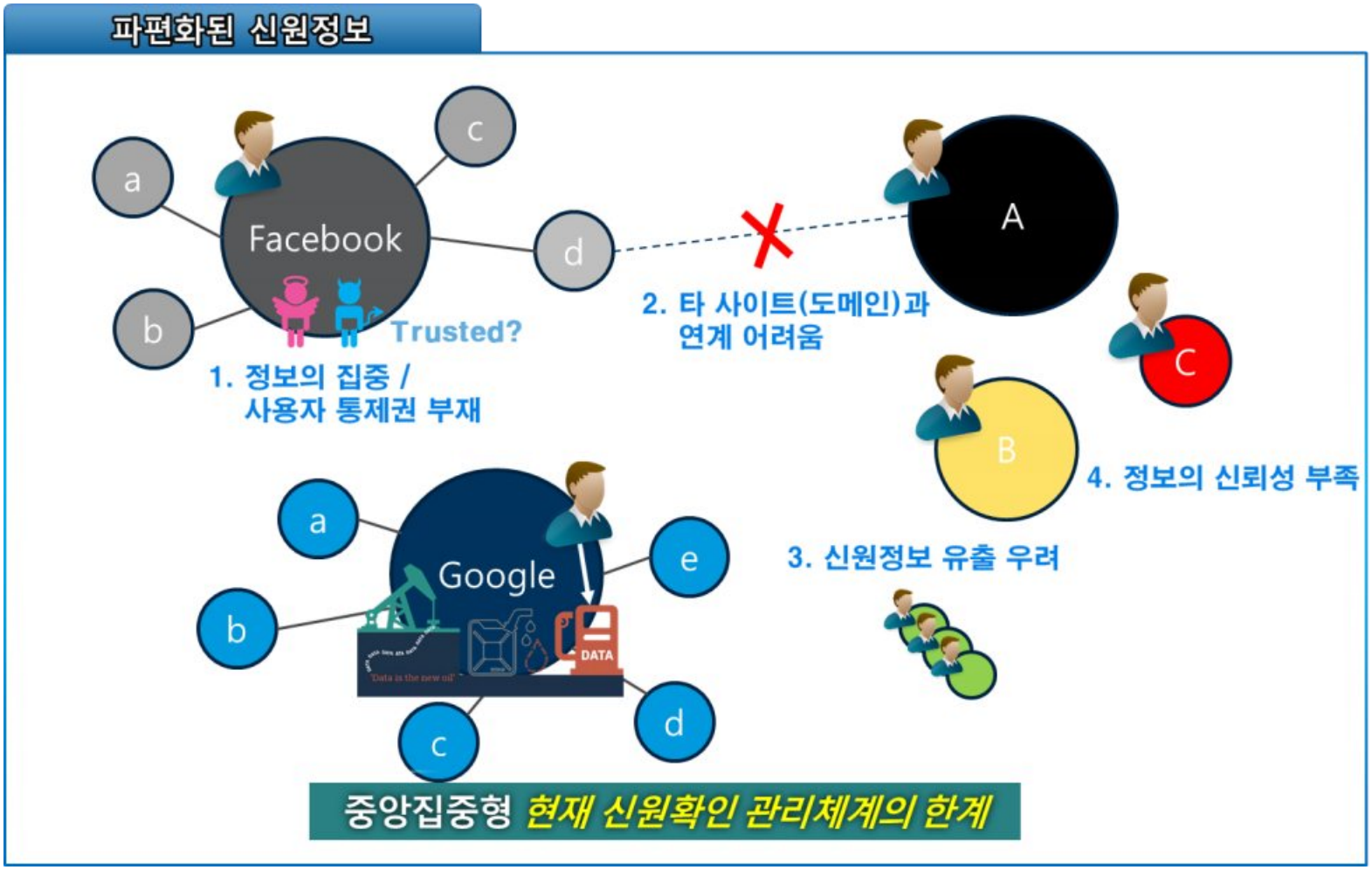
인터넷 뱅킹(고부가) 서비스

스마트 서비스

신원 확인/관리 기술의 발전 방향

2. 기술의 배경

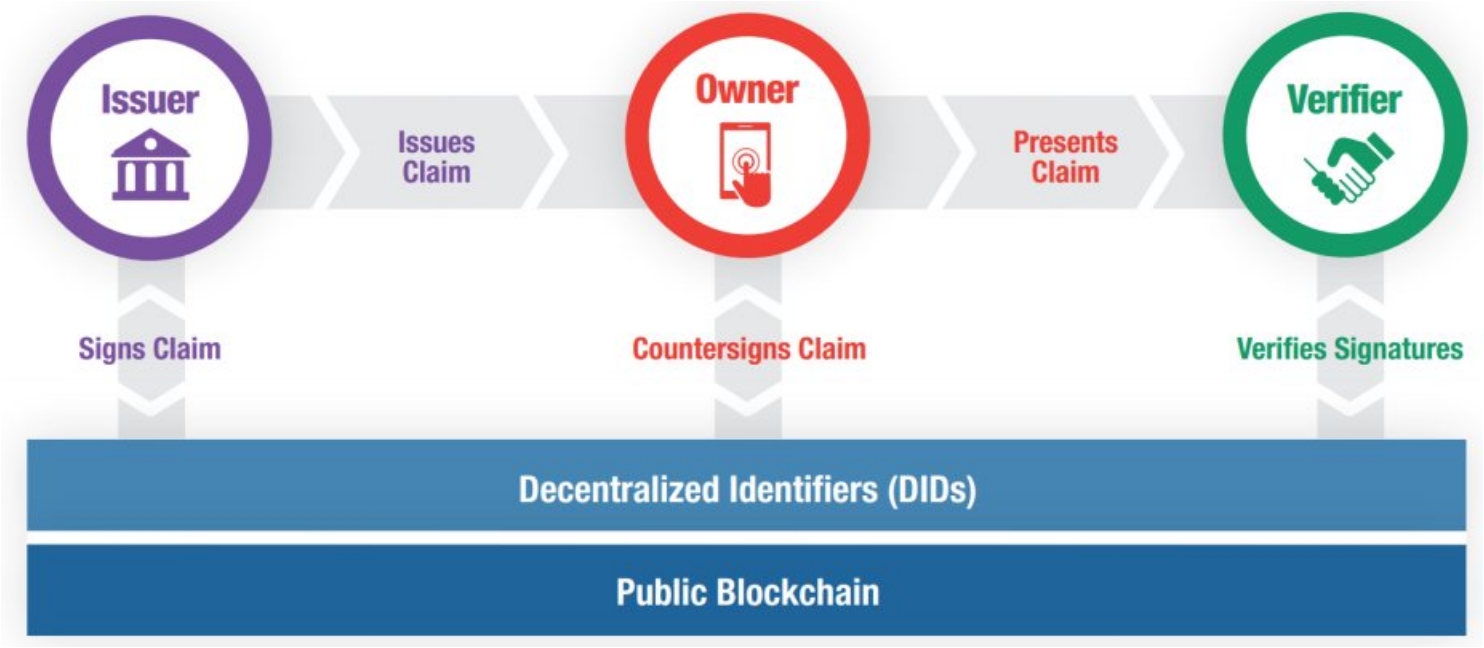
▣ 현재 신원관리 기술의 한계



2. 기술의 배경

▣ 분산ID 신원관리 기술

- ❖ 중앙 시스템에 의하여 통제 받지 않고, 사용자 스스로 식별자를 생성하고 관리함
- ❖ 자신의 신원 정보에 대한 통제권을 제3자에게 증명할 수 있음

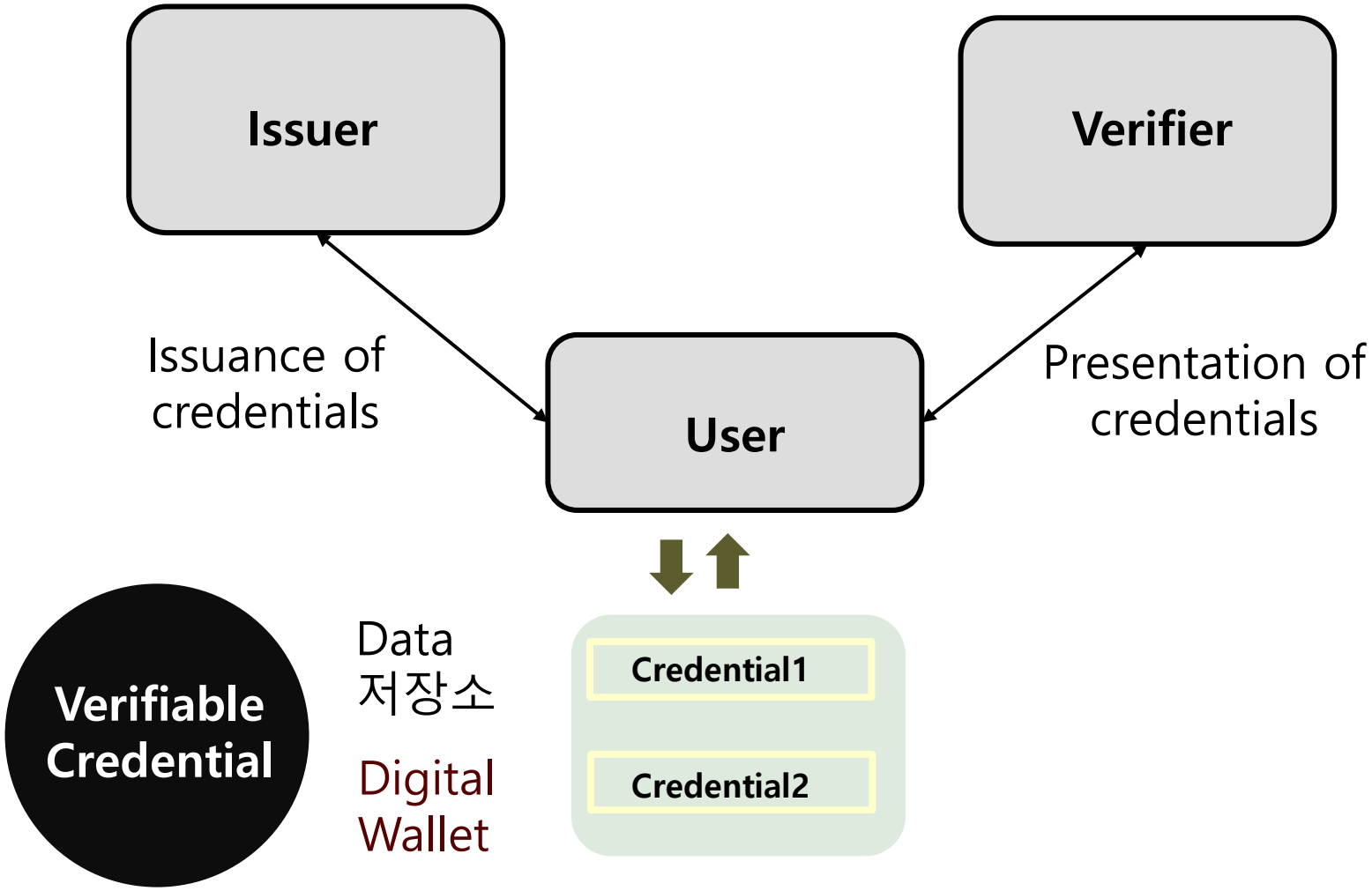


출처: Sovrin

<분산 ID 기반의 시스템 구성도>

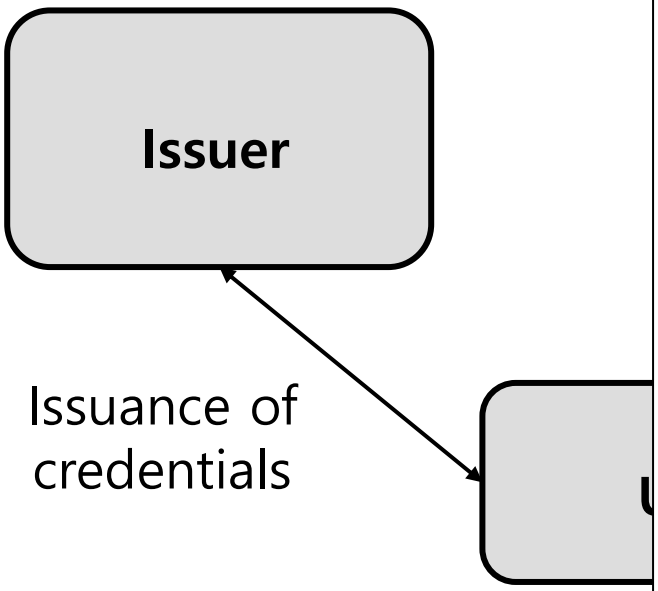
2. 기술의 배경

▣ 분산ID 신원관리 기술의 기본 구성



2. 기술의 배경

▣ 분산ID 신원관리 기술의 한계



Data 저장소

Digital Wallet

VC 예시

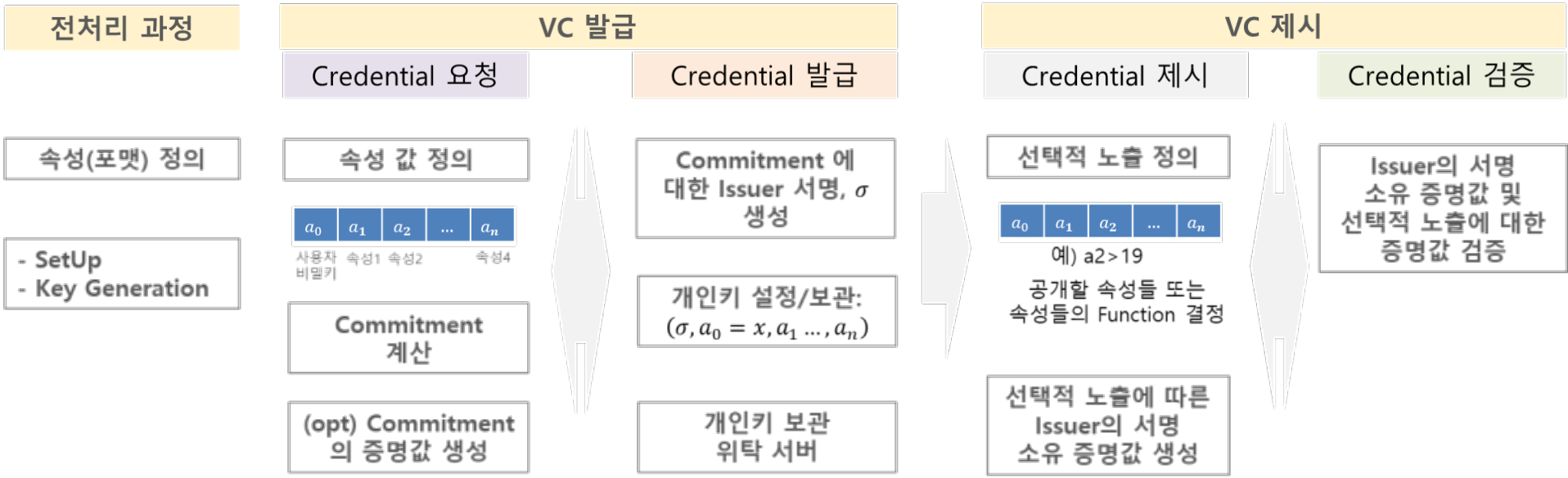

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "credentialSchema": {
    "id":"did:example:cdf:35LB7w9ueWbagPL94T9bMLtyXDj9pX5o",
    "type":"did:example:schema:22KpkXgecryx9k7N6XN1QoN3gXwBkSU8Sfy
    yYQG"
  },
  "credentialStatus": {
    "id":"https://card.com/status/24",
    "type":"CredentialStatusList2017"
  },
  "credentialSubject": {
    "CP":"010-1234-1234",
    "address": {
      "city":"Daejeon",
      "detail":"218 Gajeong-ro, Yuseong-gu ETRI",
      "zipcode":"34219"
    },
    "birthdate":"20000101",
    "card": {
      "cardExpirationDate":"20221008",
      "cardNumber":"1234-5678-9012-3456",
      "cardissuer":"BC"
    },
    "credentialInfo":"http://card.com/credential/information/xxxx"
    ,
    "gender":"M",
    "id":"did:eid:att1234567890att",
    "name":"hong gil dong"
  },
  "expirationDate":"2019-12-31T19:23:23Z",
  "id":"http://card.com/credentials/1872",
  "issuanceDate":"2019-01-01T19:23:24Z",
  "issuer":"https://card.com/issuers/832549",
  "issuerInfo":"http://card.com/issuers/information/xxxx",
  "proof": {
    "attributes":"pPYmqDvwwWBDPNykXVrBtKdsJDeZUGFA...tTERiLqsZ5oxC
    oCSodPQaggkDJy",
```


개인정보 노출
➔ 프라이버시 침해

3. 기술이전 내용 및 범위

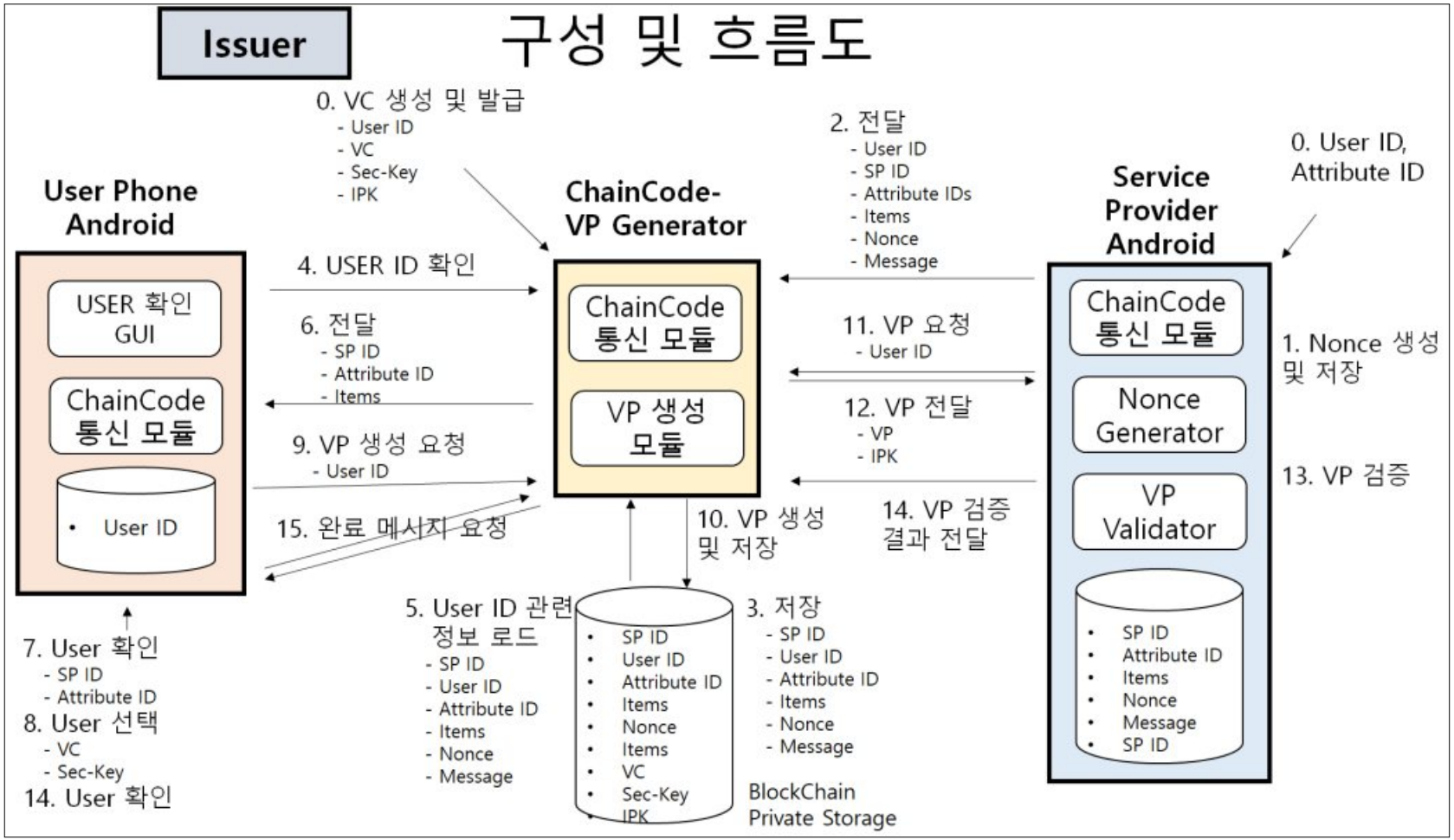
▣ 기술이전 기술 리뷰

❖ 분산ID 신원관리 기술의 신원자격 내, 개인정보에 대한 프라이버시 보호를 위한 선택적 속성 정보 노출/은닉 기능 제공



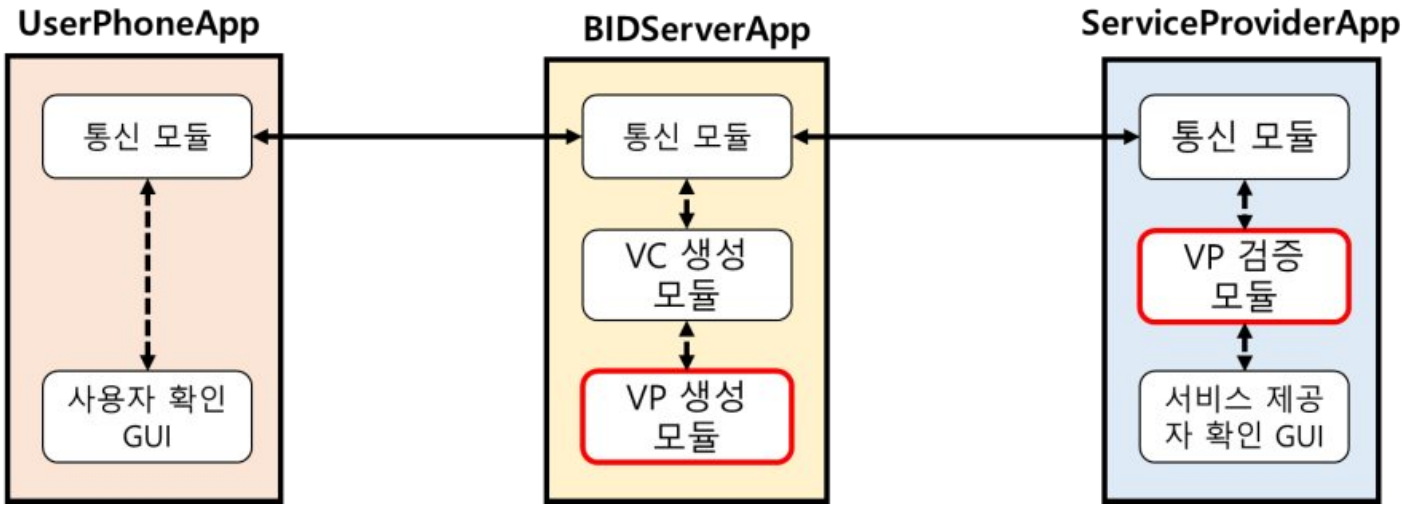
3. 기술이전 내용 및 범위

▣ 기술이전 기술 테스트 환경 및 흐름도



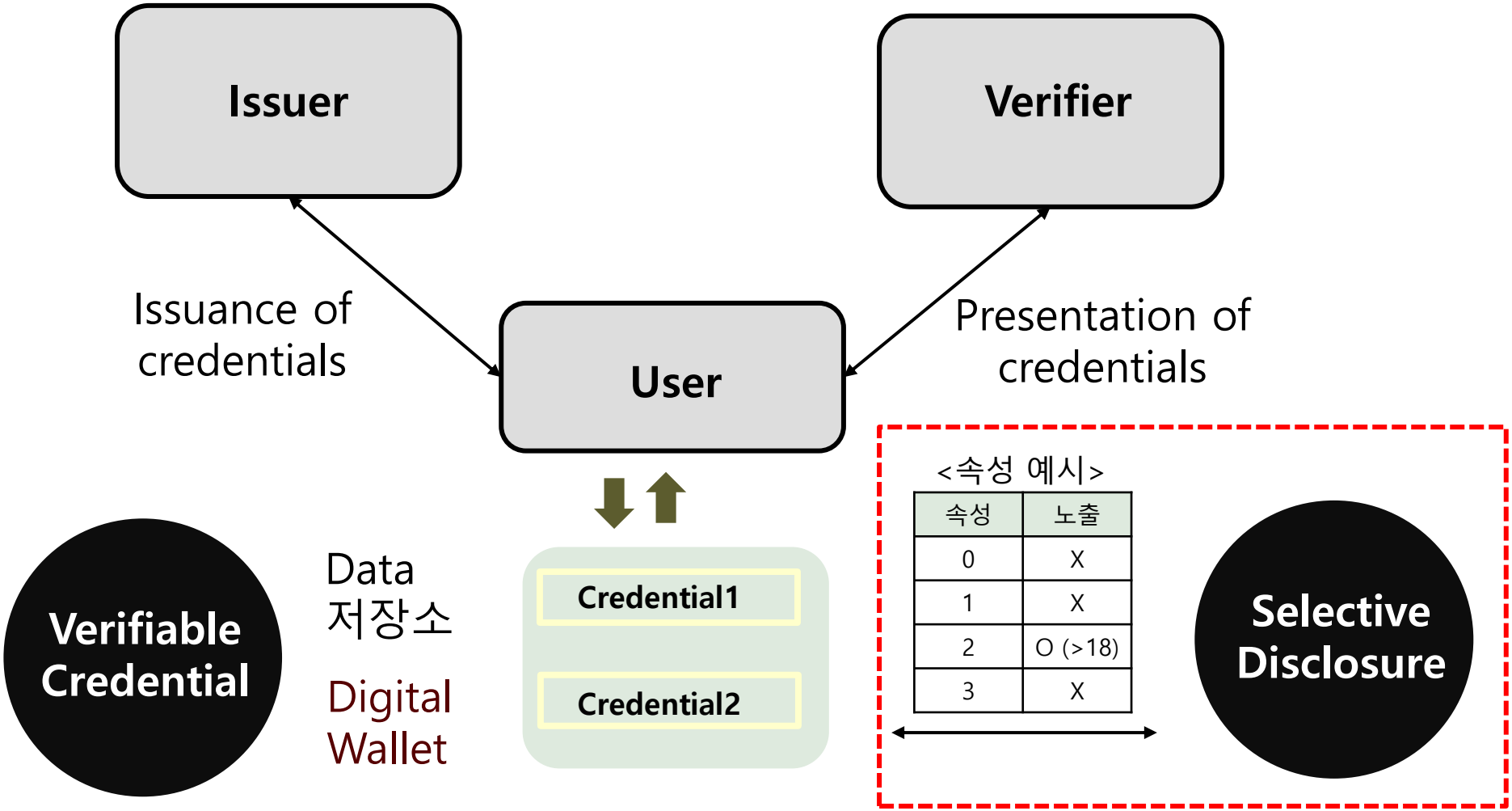
▣ 기술이전 내용 및 범위

- ❖ (익명)VP 생성 모듈
- ❖ (익명)VP 검증 모듈



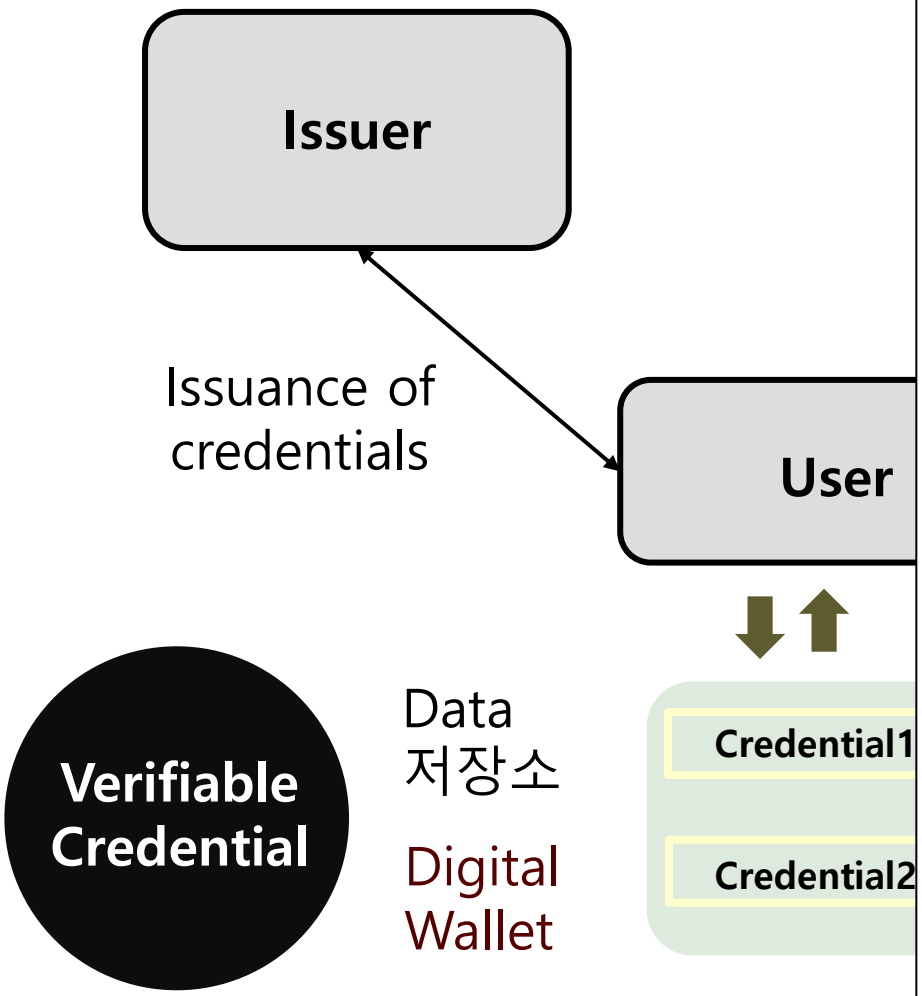
3. 기술이전 내용 및 범위

▣분산ID 신원관리 기술에 프라이버시 보호 제공



3. 기술이전 내용 및 범위

▣분산ID 신원관리 기술에



VP 예시


```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "type":"VerifiablePresentation",
  "verifiableCredential": [
    {
      "@context": [
        "https://www.w3.org/2018/credentials/v1",
        "https://www.w3.org/2018/credentials/examples/v1"
      ],
      "id":"http://card.com/credentials/1872",
      "type": [
        "VerifiableCredential",
        "PriInfoCredential"
      ],
      "credentialSchema": {
        "id":"did:example:cdf:35LB7w9ueWbagPL94T9bMLtyXDj9pX5o",
        "type":"did:example:schema:22KpkXgecryx9k7N6XN1QoN3gXwBk
        SU8SfyyYQG"
      },
      "issuer":"https://card.com/issuers/832549",
      "credentialStatus": {
        "id":"https://card.com/status/24",
        "type":"CredentialStatusList2017"
      },
      "proof": {
        "type":"AnonCredDerivedCredentialv1",
        "primaryProof":"A/5cp/+XoUkEP9pddLwur9T/DcNB+XG4Im/FpLVd
        ZV3+PhCSDGLb5xF/tOyIcGm3CjcMPhLanKNysB6PlbQYkjVlRadznp4A
        wXqJWiwavFkOkkqecd+XC7JLu91Ir6WbTceblm9JfA7S8EVweq81x8JG
        rLYUh17nentfshDGhUxtMvaYbGhixOTLt7moJeu0cObunoJyxBGkwZJ1
        6uIDcdByjjIf0qE8S4PM7ySsGJOnIWK6EtFESE6Fbt1EfdPBRTshPD4/
        DaW0n2c/5QtkXMF0ShMdIzFKQvjnh42wOENdSnibBjjFzyOmA+7cMnsu
        wxSiv87vGCBpQCs019TtAtTHojRCkzO+cz+u5RozVl4TxmIK3cJtlt5w
        P1nRrwf2vEQDLMX7nMkH8mklWm6n0/nulzsBeCMUwQSPV1AkbKenSrUZ
        UkL/IeRxmcq1+7PVVwKSq+dhdb45qtgpBWsJB4T23Z+SAqRqe16mhyCr
```


개인정보 은닉

2. 기술이전 내용 및 범위

▣ 기술 개발 현황

❖ 기술성숙도(TRL : Technology Readiness Level) 단계 : (5)단계

구 분	단계	정 의	세 부 설 명
기초 연구 단계	1	기초 이론/실험	▪기초이론 정립 단계
	2	실용 목적의 아이디어 특허 등 개념정립	▪기술개발 개념 정립 및 아이디어에 대한 특허 출원 단계
실험 단계	3	실험실 규모의 기본성능 검증	▪실험실 환경에서 실험 또는 전산 시뮬레이션을 통해 기본성능이 검증될 수 있는 단계 ▪개발하려는 부품/시스템의 기본 설계도면을 확보하는 단계
	4	실험실 규모의 소재/부품/시스템 핵심성능 평가	▪시험샘플을 제작하여 핵심성능에 대한 평가가 완료된 단계 ▪3단계에서 도출된 다양한 결과 중에서 최적의 결과를 선택하려는 단계 ▪컴퓨터 모사가 가능한 경우 최적화를 완료하는 단계
시작품 단계	5	확정된 소재/부품/시스템 시작품 제작 및 성능 평가	▪확정된 소재/부품/시스템의 실험실 시작품 제작 및 성능 평가가 완료된 단계 ▪개발 대상의 생산을 고려하여 설계하나 실제 제작한 시작품 샘플은 1~수개 미만인 단계 ▪경제성을 고려하지 않고 기술의 핵심성능으로만 볼 때, 실제로 판매가 될 수 있는 정도로 목표 성능을 달성한 단계
	6	파일롯 규모 시작품 제작 및 성능 평가	▪파일롯 규모(복수 개~양산규모의 1/10정도)의 시작품 제작 및 평가가 완료된 단계 ▪파일롯 규모 생산품에 대해 생산량, 생산용량, 불량률 등 제시 ▪파일롯 생산을 위한 대규모 투자가 동반되는 단계 ▪생산기업이 수요기업 적용환경에 유사하게 자체 현장테스트를 실시하여 목표 성능을 만족시킨 단계 ▪성능 평가 결과에 대해 가능하면 공인인증 기관의 성적서 확보
실용화 단계	7	신뢰성평가 및 수요기업 평가	▪실제 환경에서 성능 검증이 이루어지는 단계 ▪부품 및 소재개발의 경우 수요업체에서 직접 파일롯 시작품을 현장 평가(성능 및 신뢰성 평가) ▪가능하면 인증기관의 신뢰성 평가 결과 제출
	8	시제품 인증 및 표준화	▪표준화 및 인허가 취득 단계
사업화	9	사업화	▪본격적인 양산 및 사업화 단계 ▪6-시그마 등 품질관리가 중요한 단계

4. 기술의 사업성

활용 분야

▶ 프라이버시 보호가 필요한 디지털 신원정보 기반의 다양한 서비스 분야에 활용 가능

- 디지털 신원정보 관리 서비스 (모바일 신분증, 증명서 등)
- IoT 디바이스에 대한 식별 및 자격 관리 서비스 (디바이스 신원증명 등)

모바일 신분증

출처: 디지털타임즈

디바이스 자율거래

시장성

단위: 억달러

예상제품	시장	2021	2023	2025
분산ID 관련 서비스	글로벌	101	141	252

※ 글로벌 시장: 시온 리프트와 포천 비즈니스 인사이트는 DID 산업이 연평균 26%씩 성장해 2025년 252억달러(한화 29조원) 규모의 시장을 형성할 것으로 전망, 아주경제, 2020.04

※ 국내 시장: 현재 시범사업이 구축되는 정도이며, 향후 전자서명 시장과 모바일 신분증 및 증명서 시장의 일정 부분을 차지할 것으로 전망, 2019년 공인/사설 인증 서비스 시장 규모가 661억 원 규모로 추산, Itdaily, 2020.07

감사합니다.

www.etri.re.kr