https://doi.org/10.7840/kics.2022.47.10.1606

분산신원증명(DID)과 공개 키 기반(PKI) 간 상호운용가능한 신뢰연결 프레임워크 기본모델 제안

이 강 효◆, 박 소 현*, 김 현 준*, 하 태 균*, 유 주 열**, 김 경 백°

A Proposal of an Inter-Operable Trust Anchor Framework Basic Model for Decentralized Identity (DID) and Public Key Infrastructure (PKI)

Kanghyo Lee◆, So-Hyeon Park*, Hyunjun Kim*, Tae Gyun Ha*, Yoo Joo Yeol**, Kyungbaek Kim°

요 약

최근 정부의 모바일 운전면허증, 백신접종증명서비스 등 자기주권을 사용자에게 보장하는 분산신원증명(Decentralized ID) 기술을 활용한 서비스가 점차 나타나고 있다. DID는 데이터의 자기주권을 사용자에게 보장하고 데이터를 여러 분야에 안전하고 유연하게 제공할 수 있는 새로운 신원확인체계이다. 하지만, DID 생태계는 초기 수준으로 사용자가 자신의 데이터 통제권을 보장하고, DID와 기존 PKI 기반의 전자서명 서비스 간 상호운용을 보장하기 위한 프레임워크가 부재하다. 이에 발행기관(issuer), 사용자(holder), 검증기관(verifier) 등 DID 참여자 모두가 신뢰할 수 있는 프레임워크 기본모델을 제안하여 강건한(robust) DID 생태계를 마련할 필요가 있다. 또한, 사용자가 안전하고 편리하게 신원확인서비스를 이용하기 위해서는 정부에서 최소한의 신뢰성을 보증해야 한다. 이는 신뢰연결(Trust Anchor) 프레임워크 기본모델로 보완할 수 있으나, 다양한 방법론이 존재한다. 이 논문에서는 분산신원증명과 공개 키 기반 구조 간 상호운영이 가능한 신뢰연결 체계를 구축하기 위한 기본모델을 제안한다. 제안한 신뢰연결 프레임워크 기본모델은 신원확인을 넘어서 다양한 스마트 기기 등 사물에 적용할 수 있는 미래형 인증서비스로 중요한 역할을 할 것으로 기대한다.

키워드 : 블록체인, 분산신원증명, 자기주권신원, 신뢰연결, 프레임워크
Key Words : Blockchain, Decentralized Identity, DID, Self-Sorverign Identity, SSI, Trust Anchor, Framework

ABSTRACT

Recently, services using distributed identification (DID) technology that guarantee data sovereignty to users, such as the government's mobile driver's license and vaccination certificate service, are gradually appearing. However, the DID ecosystem is at an initial level, and there is no framework to guarantee users' control over their data and interoperability between DID and the existing PKI-based digital signature service. In this regard, we intend to prepare a robust DID ecosystem by proposing a framework basic model that all DID participants,

※ 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 지역지능화혁신인재양성사업의 연구결과로 수행되었음(IITP-2022-RS-2022-00156287)
◆ First Author : Korea Internet & Security Agency, Chonnam National University, kanghyo.lee@kisa.or.kr, 정회원
° Corresponding Author : Chonnam National University, kyungbaekkim@jnu.ac.kr, 종신회원
* Korea Internet & Security Agency, Chonnam National University, sohyeon@kisa.or.kr; hyunjun@kisa.or.kr; niceha@kisa.or.kr
** Korea Internet & Security Agency, jyyoo@kisa.or.kr
논문번호 : 202205-077-C-RE, Received April 30, 2022; Revised July 26, 2022; Accepted August 8, 2022

such as issuers, holders, and verifiers, can trust. DID is a new identity verification system that guarantees self-sovereignty to users and can provide data safely and flexibly across fields. In order for users to safely and conveniently use the identity verification service, the government must guarantee the minimum reliability. This can be supplemented with the Trust Anchor model, and there are various methodologies. The trust connection framework basic model proposed in this paper is a policy model that can be the basis for service activation. It aims to contribute to establishing a trust connection system through the basic model and securing interoperability and reliability between DID and PKI services.

Ⅰ. 서 론

최근 개인정보보호위원회에 따르면 2019년 한 해 동안 개인정보 침해 신고센터에 접수된 15만 9,255건의 신고·상담 건 가운데 가장 큰 비중을 차지한 개인정보 침해 유형은 '주민등록번호 등 타인정보의 훼손·침해·도용'으로 전체의 84%로 13만 4,000여 건을 차지했다[1]. 국내 최대 규모의 온라인 커뮤니티는 개인정보 유출, 도용 등 기업의 개인정보 보유로 인한 사회적 문제가 증가하기 때문에 가입자의 이름, 이메일 주소 등 모든 개인정보를 일괄 파기했다. 이는 사용자의 자기주권을 보장하고, 기업은 관리해야하는 사회적 문제를 최소화하기 위한 움직임이다.

이에 신원인증 모델도 개별 신원 모델에서 연합형 신원 모델, 자기주권신원(Self-Sovereign Identity, SSI) 모델로 변모하고 있다. 이 모델은 정보주체가 자신의 정보를 소유, 이동, 공개 등 직접 제어할 수 있다. 신원정보 제공기관 또는 인증기관에 의존하지 않고, 정보주체가 직접 관리할 수 있는 탈중앙화된 신원 관리체계이며, 이를 구현한 기술이 DID(Decentralized ID, DID)이다. DID는 오프라인에서 신분증을 꺼내어 신원확인을 관리하는 것처럼 온라인에서 사용자 스스로 자신의 신원정보를 선택하여 일부만 제출할 수 있는 등 관리 및 통제할 수 있다.

DID는 가트너(Gartner)의 "블록체인 기술 하이프 싸이클(Hype cycle)"에서 부풀려진 기대의 정점(Peak of Inflated Expectations)에 위치한다[2]. 또한, 글로벌 시장조사기관인 테크나비오(technavio)에 따르면 글로벌 신원관리 시장 전망은 '20년부터 '25년까지 25억 8000만 달러로 성장할 전망이며, 향후 연평균성장률은 70.8%에 달할 것으로 전망했다[3].

국내는 모바일 운전면허증, 백신접종증명서비스 등 다양한 분야에서 자기주권을 사용자에게 보장하기 위한 목적으로 DID를 도입하는 활용사례가 점차 증가하고 있다. 하지만, 초기시장인 DID는 디지털 방식의 신뢰연결 프레임워크가 부재하여 서로 다른 서비스 간 증명서 발급 및 제출이 제한적이다. 이에 발행기관(issuer), 사용자(holder), 검증기관(verifier) 등 DID 참여자 모두가 신뢰할 수 있고, 기존 PKI와 상호운용할 수 있는 강건한(robust) DID 생태계 구축이 필요하다. 이에 본 논문에서는 DID 및 PKI 간 상호운용 가능한 신뢰연결 프레임워크 기본모델을 제안한다.

본 논문의 구성은 2장에서 블록체인, DID 등 배경지식을 설명하고, 3장에서는 DID 관련 해외정책 사례를 살펴보고, 4장에서는 국내의 신뢰연결 프레임워크 설계 시 고려사항을 검토한 후 5장에서 신뢰연결 프레임워크 기본모델을 제안하고, 마지막으로 6장에서 결언을 맺는다.

Ⅱ. 배경지식

2.1 블록체인(Blockchain)

비트코인의 경우 P2P 타임스탬프(timestamp) 서버에 사용되지 않은 트랙잭션(Unspent Transaction Output, UTXO)을 남긴다[4]. 이때 일정 크기의 데이터를 나누어 '블록(block)'이라는 단위로 저장하고, 시간 순서대로 '연결(chain)'하는 개념을 일컬어 '블록체인'이라 부른다. 블록체인은 신뢰할 수 있는 제3자(Trusted Third Party, TTP) 없이도 기존 서비스를 동일하게 구현할 수 있다.

블록체인 참여자는 블록에 거래내역(transaction) 또는 프로그램 코드를 포함시켜 블록체인에 전파될 후보 블록을 생성한다. 참여자들은 합의 알고리즘(consensus algorithm)에 따라 후보블록(candidate block) 중 하나의 블록을 선택하여 참여자 모두에게 전파하고 서로가 검증한다. 문제가 없다면 불변성(finality)을 확정하고 블록체인에 기록한다. 참여자들은 블록체인에 기록된 데이터를 서로 감시하여 위변조에 안전하다.

비트코인의 스크립트 언어에서 벗어나 튜링완전(turing completeness)한 이더리움이 등장했다[5]. 이더리움은 블록체인 네트워크가 하나의 컴퓨터처럼 동작

하기에 월드컴퓨터(world computer)라 정의했고, 이때 실행되는 프로그램 코드가 스마트컨트랙트(smart contract)이다.

2.2 분산신원증명(DID)

DID는 개인정보에 대한 통제권을 서비스 기업에서 개인에게 돌려주어 자기주권을 보장한다[6]. DID는 사용자가 신분증, 증명서 등을 모바일 기기에 저장하고, 상황에 따라 필요한 개인정보를 선택하여 제출할 수 있다.

DID 서비스의 참여자는 [그림 1]과 같이 크게 발행기관, 사용자, 검증기관으로 구분된다[7]. 사용자는 모바일 기기의 전자지갑 앱을 통해 개인정보를 직접 관리한다. 발행기관은 사용자가 신분증, 증명서를 발행을 요청할 경우, 사용자를 검증한 후 요청자료를 발행한다. 검증기관은 서비스 제공을 하는 기업이나 기관이며, 사용자가 제출한 신분증 또는 증명서를 검증한 후 서비스를 제공한다[8].

이를 구현하기 위해서 탈중앙화 환경에서 전자서명하고 검증할 수 있는 탈중앙화된 PKI(Decentralized PKI, DPKI) 기술을 활용한다. DPKI는 [표 1]과 같이 기존 PKI와 달리 인증서 없이 블록체인에 저장되어 있는 DID 문서(DID Document)를 불러옴으로써 검증이 가능하다. DID 문서에는 DID 식별자에 해당하는 공개키 정보, 암호알고리즘, 생성시간 등 검증 관련 메타데이터가 저장되어 있다. 또한, DID 식별자(Decentralized Identifiers, DIDs)는 URN(Universal Resource Name) 규격으로 이루어져 있으며, [그림 2]와 같이 DID 스킴(DID Scheme), DID 메소드(DID Method)와 세부식별값으로 구성된다[9]. 특히, DID 메소드는 DID 정보를 찾아갈 때 우선적으로 확인하는 값이며, 메소드에는 DID를 생성(Create)하고, 읽고(Read), 갱신(Update)하고, 삭제(Delete)할 때의 기술규격이 정의되어있다. 발행기관이 사용자에게, 사용자가 검증기관에 제출하는 증명서를 각각 VC(Verifiable Credential), VP(Verifiable Presentation)라 부른다[7]. 또한, VP는 여러 VC의 정보를 결합하여 제출할 수 있다. DID 동작방식은 다음과 같다[7].

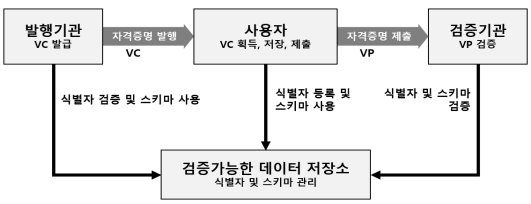
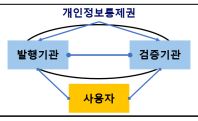
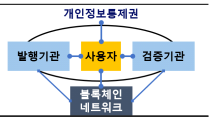


그림 1. W3C의 Verifiable Credentials Data Model
Fig. 1. Verifiable Credentials Data Model of W3C

표 1. PKI 및 DPKI 비교
Table 1. Compare PKI with DPKI

구분	인증서 기반 PKI	블록체인 기반 DPKI
형태	중앙집중형(인증기관)	탈중앙형
주체 및 공개키 바인딩	주체의 공개키에 인증기관이 자신의 개인키로 전자서명한 "인증서" 형태로 생성	블록체인에 주체의 식별자(DID)와 공개키를 포함하는 "DID문서" 저장
보관 방식	각 주체가 자신의 인증서를 각자 보관	블록체인 상에 모든 주체의 DID 문서 기록
배포 방식	전자서명 생성 시 인증서도 검증기관에 전송	검증기관은 블록체인에서 주체의 DID 문서를 스스로 조회
자기주권 신원지원	△ ※서비스 유형 및 구현 방식에 따라 일부 가능	○
단일점 실패 방지	×	○
구성안		

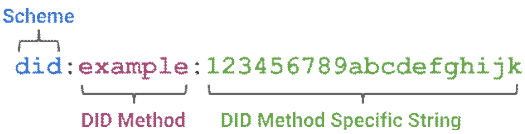


그림 2. 분산식별자 구조
Fig. 2. Structure of Decentralized Identifier

1) 사용자가 모바일 전자지갑 앱을 설치하면 자동으로 분산식별자를 부여받고, 이에 대응하는 DID 문서가 블록체인에는 저장된다.
2) 사용자는 발행기관에 자격증 발급을 요청하며, 발행기관은 해당사실을 확인한 후 전자서명한 VC를 발급한다.
3) 사용자는 다수의 VC를 전자지갑 앱을 통해 관리한다.
4) 사용자는 서비스 이용을 목적으로 신원 또는 자격증명을 해야할 때, 전자지갑 앱의 VC 중 민감하지 않은 정보만을 선택하여 검증기관에 전자서명한 VP를 제출한다.
5) 검증기관은 사용자가 제출한 VP로부터 사용자 분산식별자를 확인하여 사용자의 DID 문서를 불러와 사용자의 전자서명을 검증한다. 발행기관의 전자서명도 동일하게 검증한다.

DID는 각 증명서의 정보(claim)를 선택적으로 제출할 수 있으며, 정보와 정보의 관계를 증명서에 포함할 수 있다는 점이 특징이다. DID는 모바일 운전면허증, 백신접종증명확인 서비스 등에 적용되어 있다[10,11].

Ⅲ. 해외정책 분석

유럽연합 등 해외국과 ToIP, Sovrin 등 DID 개념화, 기술구현 등을 주도하는 커뮤니티에서는 신뢰목록 관리, 발행권한 부여 등 발행기관에 대한 신뢰를 부여하고자 프레임워크를 개발하고 있다. 본 장에서는 DID 신뢰 프레임워크 사례를 살펴보고자 한다.

3.1 eIDAS(electronic IDentification and trust services)

유럽연합(EU)는 전자적 거래를 위한 전자적 신원확인 및 신뢰서비스 법안(eIDAS)을 시행했다[12]. 해당 법안은 EU 내수시장에서의 전자거래를 위한 전자신원확인 및 인증 업무에 관한 규정으로 개별 회원국의 전자신원확인 체계에서 발급되는 다양한 ID 간의 상호 효력을 인정한다. 동 규칙은 기업, 시민, 공공기관 간의 안전하고 원활한 전자적 상호작용을 가능하게 하는 eID(electronic identification, eID) 체계를 보장하며, EU 회원국 간 전자신원확인이 상호인정되는 환경을 제공한다[13].

eID는 온라인상에서 유럽시민 개인과 기업이 신원을 증명할 수 있는 전자신분증 솔루션을 의미한다. eID는 온라인 서비스에 안전하게 접근하고 안전한 방식으로 전자 거래를 수행할 수 있게 해주는 신원 확인 솔루션으로서, 신원을 확실하게 보장하고 자격을 갖춘 사람에게 온라인 공공서비스를 제공할 수 있도록 지원한다. eID는 네덜란드, 영국, 스위스 등 32개 유럽 국가들이 이용하고 있다[13].

eIDAS 시행으로 EU 내에서는 통일된 양식의 한 가지 서명으로 정확하고 안전한 거래가 가능해짐에 따라 EU 내 각국에서는 고지된 eID에 대한 상호인증을 의무화했다. EU에서는 3가지 형태의 전자서명을 인정하고 있으며, 모두 법적 효력을 부여했다[14].

- Basic E-Signature : 단지 서명자 본인인지를 여권이나 신분증을 통해 확인
- Advanced E-Signature : 별도의 본인인증절차를 걸쳐 서명자 본인 확인
- Qualified E-Signature : 제3의 신용서비스 제공자 (Trust Service Provider)를 통한 본인 확인

3.1.1 EBSI(European Blockchain Services Infrastructure)

EBSI는 블록체인 기술을 활용하여 국경을 넘는 공공서비스를 제공하기 위해서 유럽 전역에 노드를 분산·연결한 네트워크이다[15]. 유럽연합 국가들은 EBSI를 구축하기 위해서 상호협력하기로 선언하고, 블록체인 파트너쉽에 서명했다[16]. 이는 [표 2]와 같이 유럽연결기구(Connecting European Facility, CEF) 디지털에서 구축하려는 구성요소 중 하나이다[15].

EBSI는 유즈케이스, 코어서비스, 체인 및 스토리지, 인프라 등 총 4계층으로 구성된다[17].

- 유즈케이스 계층 : 디앱 샌드박스, 디앱 양식(DApp Template) 등 서비스 구현 시 참고할 수 있는 샘플 애플리케이션, 실험환경 등을 제공
- 코어서비스 계층 : EBSI 5대 원칙을 준수하면서, 외부 인터페이스와 상호운용하고 DID, 전자서명 등을 검증하기 위해서 개인데이터지갑, eDIAS 서명 서비스, 유니버셜 DID 리졸버, 학위증 증명, 자기주권신원, 문서 공증 서비스 등 핵심 기능을 제공
- 체인 및 스토리지 계층 : 이더리움 엔터프라이즈, 하이퍼레저 패브릭 등 정부가 호스팅하는 블록체인과 분산DB, 분산파일시스템 등 정부가 호스팅하는 오프체인 저장소를 제공
- 인프라 계층 : 네트워크, 컴퓨팅, 배포 기능을 포함하여 EBSI 노드를 설정하는데 필요한 모든 인프라 요소를 나타냄

표 2. CEF DIGITAL 구성요소(Building Blocks)
Table 2. CEF Digital Building Blocks

구분	내용
Blockchain	블록체인 인프라(EBSI)
eID	전자신분증 및 증명서
eDelivery	문서 및 데이터 수집·유통
eSignature	전자서명 생성 및 검증
eInvocing	전자 인보이스
eTranslation	전자번역
eArchiving	디지털 정보 저장 보관
Context Broker	실시간 데이터 수집·유통
Once-only Principle	개인·기업에서 정보 1회 접근
Big Data Test Infrastructure	안전환경에서 빅데이터 실험

표 3. EBSI 5대 원칙
Table 3. The five key principles of EBSI

구분	내용
공공재	EBSI 관리는 공익을 위해 이루어져야 하며, 전체 회원국 시민에게 공익제공을 목적으로 공공·민간 서비스 사용을 제한할 책임이 있음
거버넌스	EBSI 거버넌스 시스템은 이해관계자 간 합의를 통해 의사결정에 도달해야 함
조화	EBSI 거버넌스는 지원프로토콜 확산 또는 아키텍처 충돌을 방지하기 위한 기술요구사항 및 아키텍처 간의 조화를 장려하고 유지해야 함
오픈소스	가능하면 모든 EBSI 서비스 및 구조에 대한 개발은 민간부분(서비스 제공업체, 공급업체 등) 건전한 경쟁을 가능하도록 오픈소스여야 함
EU 가치	EBSI는 GDPR 및 eIDAS 등 규정을 준수해야 함

3.1.2 ESSIF(European Self-Sovereign Identity Framework)

ESSIF는 EBSI를 활용하여 구축한 적용사례 중 하나이다. ESSIF는 유럽시민이 중앙집중식 당국에 의존하지 않고도 국경을 넘어 자신의 신원을 생성하고 제어할 수 있는 SSI 기능을 구현하는 것을 목표로 한다[18]. 자연인 또는 법인의 신원에 중점을 둔 EBSI 인프라를 기반으로 필요한 자원기능을 제공하기 위한 프레임워크이다. ESSIF는 EU 기업이 VC를 취득하고, 검증 가능한 명령·협의서를 등록하며, 검증가능한 주장을 취득할 수 있도록 허용할 것이며, 이는 의존하는 당사자를 식별·인증하고 필요한 청구·참고를 제공하는 데 사용한다.

3.2 ToIP(Trust over Internet Protocol)

ToIP는 리눅스 재단(Linux Foundtaion)의 글로벌 오픈소스 생태계 프로젝트 중 하나이며, [그림 3]과 같이 ToIP는 기술과 거버넌스로 구분된 이중 스택으로 구성된다[19]. 특히, ToIP는 DID와 VC를 개발하던 개발자 커뮤니티에서 새로운 P2P 신뢰 모델이 인터넷 규모의 디지털 신뢰 인프라를 구축할 수 있다고 내다봤다. 초기에는 기술 솔루션에 중점을 아키텍처를 설계하였으나, 실세계에 적용하기 위해서는 실용적인 거버넌스와 정책의 중요성을 인지했다.

결국, 기술 뿐만 아니라 비즈니스, 법적, 사회적 관점의 인간 신뢰를 결합한 디지털 신뢰 아키텍처를 정의하는 표준이다. 이때 1계층과 2계층은 기술 신뢰(Technical Trust)로써 서로 다른 시스템 간 안전한 비공개 연결을 설정할 수 있는 기술적 신뢰를 제공하고, 3계층과 4계층은 사람 신뢰(Human Trust)를 위해 인간의 신뢰를 생성하고 유지되도록 설계했다.

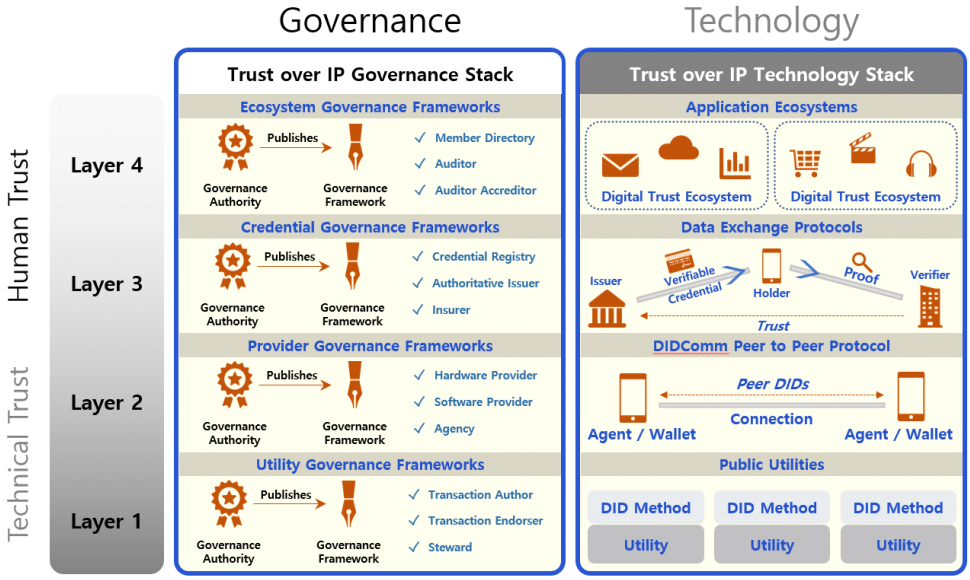


그림 3. ToIP의 이중 스택 구조
Fig. 3. Trust Over IP Dual Stack Model

3.2.1 1계층 : 공공 유틸리티

1계층 기술스택은 W3C DID 규격에 따라 블록체인 또는 다른 분산시스템에 저장된 공개키를 식별하고 검증하는 방법을 표준화한다. 이는 VC 발급자의 DID와 공개키에 대한 강력한 암호학적 신뢰를 부여할 뿐만 아니라 블록체인, 분산원장, 분산 파일 시스템, 분산 해시 테이블 등 신뢰 인프라 기술을 제공한다.

기술적 신뢰는 기계와 기계 사이에 이루어지지만, 이를 구현하기 위해서는 여전히 사람이 시스템을 설계하고, 코딩, 테스트, 인증해야 한다. 이를 위해서 1계층의 유틸리티 거버넌스 프레임워크(Utility Governance Frameworks, UGF)는 더 높은 상위 계층에서 신뢰하면서 운영·실행될 수 있는 유틸리티와 정책을 규정해야 한다.

3.2.2 2계층 : DID 통신 프로토콜

2계층은 공개 DID 또는 피어 DID를 사용하여 P2P 간 안전한 비밀통신을 연결하기 위해 필요한 전자지갑 또는 에이전트를 정의한다. DIDComm 프로토콜은 TCP/IP의 인터넷 프로토콜과 같이 ToIP에서 중요한 역할을 수행한다. 피어 DID의 경우 P2P 간 직접 교환하는 방식이므로 블록체인을 사용하지 않는다. 이는 확장성과 개인정보에 있어 상당한 이점을 가진다.

공급자 거버넌스 프레임워크(Provider Governance Frameworks, PGF)는 하드웨어 공급자, 소프트웨어 공급자 그리고 클라우드 호스팅 공급자가 인증받을 수 있는 개인정보, 보안 그리고 데이터 보호 표준을 정의한다.

3.2.3 3계층 : 데이터 교환 프로토콜

3계층 기술스택에서는 발급자, 보유자, 검증기관이 DIDComm과 같은 자격증명 교환 프로토콜을 사용하여 VC를 교환한다. 이 외에도 다양한 신뢰할 수 있는 데이터 교환 프로토콜을 구현할 수 있다.

거버넌스 스택에서는 자격증명 거버넌스 프레임워크(Credential Governance Frameworks, CGF)는 모든 디지털 자격증명을 여러 발급자가 발급하거나 다양한 검증기관이 승인하는 데 필요하다. 해당 프레임워크는 발급자가 어떤 정책에 따라 자격증명, 보증수준, 신뢰마크 등을 판단하여 사용자에게 발급할지를 정의한다.

3.2.4 4계층 : 응용 프로그램 생태계

4계층은 사람이 특정 비즈니스, 법적 또는 사회적 목적의 도움을 신뢰된 방식으로 제공받기 위해서 응용 프로그램과 상호작용한다. 응용 프로그램은 1, 2, 3계층의 프로토콜을 사용하여 DID를 등록하고, 상호 연결을 형성하고, 검증가능한 자격증명을 획득·교환한다.

생태계 거버넌스 프레임워크(Ecosystem Governance Frameworks, EGF)는 ToIP 스택의 모든 계층의 생태계를 모든 정부 기관과 정부 프레임워크에 적용할 수 있는 정책과 원칙, 목적을 정의할 수 있다. 이는 앱, 사이트 그리고 비즈니스 간에 마찰 없이 데이터를 교환하게 하며, 동시에 사용자에게 보안과 개인정보보호, 데이터 보호에 대한 일관된 경험을 제공한다.

3.3 SGF(Sovrin Governance Framework)

SGF는 자기주권신원을 위한 글로벌 공공 유틸리티인 소브린 네트워크(Sovrin network)의 법적 기반이다[20]. 전문화된 도메인별 거버넌스 프레임워크(Domain-Specific Governance Framework, DSGF)를 가진다. DSGF는 SGF에서 정의한 원칙, 정책, 용어 그리고 표준을 활용하여 각 도메인에서 고유의 디지털 자격증명을 정의하고, 발급 정책 등을 정의한다.

소브린 스택은 SSI 인프라를 4계층 스택으로 개념화하였으며, 하위 2계층은 기술적 통신, 상위 2계층은 비즈니스, 법률 등 인적 신뢰제공으로 정의했다. 이 스택은 소브린 원장, 에이전트 간 프로토콜, 자격증명 교환, 거버넌스 프레임워크 등 4계층으로 구성되었으며, 추후 ToIP 스택으로 발전했다.

SGF V2의 주요 문서 아키텍처는 [그림 4]와 같으며, SGF V2의 기본문서에는 다음을 포함한다. 각 도메인은 SGF V2의 내용을 준수하여 원칙과 정책을 생성해야 한다.

- Sovrin Governance Framework Master Document : SGF V2의 목적, 핵심원칙 및 핵심 정책을 정의
- Sovrin Glossary : 모든 SGF V2 문서와 소브린 인프라에 사용되는 용어에 대한 포괄적인 용어집과 핵심 용어 그룹에 대한 심층 설명을 제공
- Sovrin Trust Assurance Framework : SGF의 정책에 대한 다양한 소브린 행위자의 적합성을 평가하기 위한 기술과 프로세스를 정의

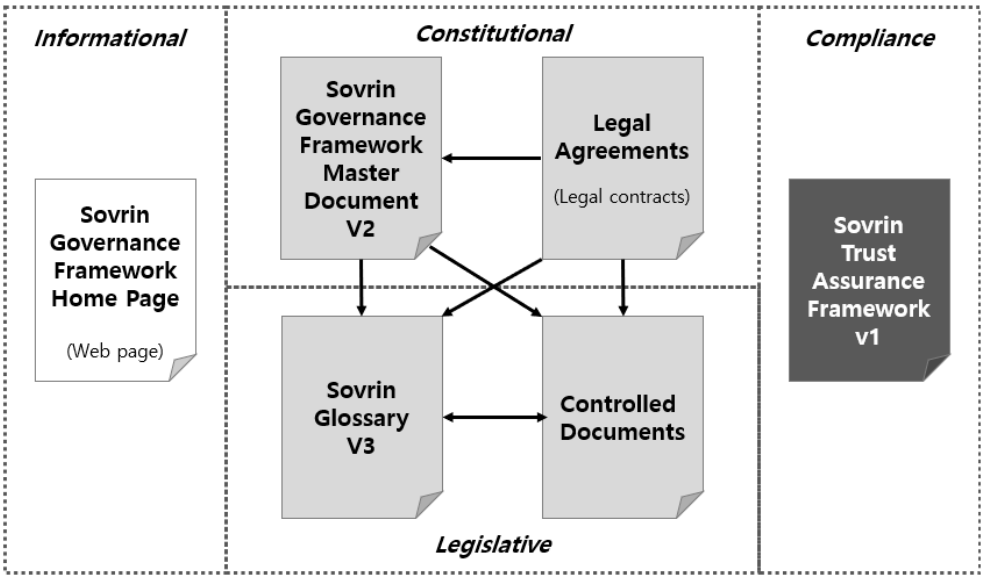


그림 4. Sovrin Governance Framework V2의 문서 아키텍처
Fig. 4. Sovrin Governance Framework V2 Master Document

SGF V2는 또한 5가지 법적 계약을 포함한다.

- Sovrin Steward Agreement : 소브린 재단과 소브린 스튜어트 간의 계약
- Steward Data Processing Agreement : GDPR과 기타 데이터 보호 규정을 준수하기 위한 각각의 책임을 설정한 소브린 재단과 소브린 스튜어트 간의 계약
- Transaction Author Agreement : 소브린 재단과 소브린 원장의 쓰기 또는 거래를 시작하는 개인 또는 기관 간의 계약
- Transaction Endorser Agreement : 소브린 재단과 소브린 원장에 대한 접근 권한을 요청하는 조직 간의 계약
- Transaction Endorser Data Processing Agreement : GDPR과 기타 데이터 보호 규정을 준수하기 위한 각각의 책임을 설정한 소브린 재단과 거래 보증인 간의 거래

마지막으로, 소브린 재단 내의 특정 하위그룹에서 관리하는 정책이 포함된다.

- Sovrin Governing Body Policies : 모든 소브린 이사회에 적용되는 거버넌스 문서
- Sovrin Ledger Access Policies : 소브린 원장에 대한 읽기, 쓰기 그리고 소브린 원장 데이터 처리를 관리하는 문서
- Sovrin Steward Business Policies : 소브린 스튜어드의 자격, 신청, 활성화, 운영, 정지 그리고 해지를 관리하는 문서
- Sovrin Steward Technical and Organization Policies : 소브린 스튜어드에 대한 보안, 노드 운영, 노드 선택 및 보고 요구사항을 관리하는 문서
- Transaction Endorser Technical and Organization Policies : 거래 보증인의 보안, 운영 정책 요구사항을 관리하는 문서
- Sovrin Economic Policies : 경제적 인센티브, 수수료 및 규정 준수를 관리하는 문서
- Sovrin Trust Mark Policies : 스튜어드, 대행사, 개발자의 소브린 신뢰 마크 사용을 관리하는 문서

SGF는 대의적인 자기주권신원의 원칙과 정책을 정의했으며, [그림 5]와 같이 각 도메인에 대한 세부적인 원칙 및 정책을 수립할 때 SGF를 준수함으로써 분야 간의 상호운용성 및 보안성을 제공할 수 있는 기본구조를 갖추게 한다.

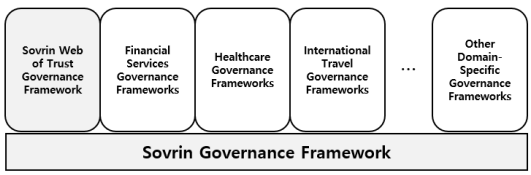


그림 5. 여러 DSGF로 구성되는 SGF
Fig. 5. SGF consisting of several DSGFs

3.4 해외 신뢰연결 프레임워크 비교

ESSIF, ToIP, SGF 등 해외 신뢰연결 프레임워크가 가지는 신뢰기관, 신뢰저장소, 서비스 주체 관점 및 기술규격 관점에서 각 모델이 가지는 특징을 비교한다.

3.4.1 신뢰 기관

신뢰기관은 각 DID 프레임워크에서 특정 검증가능한 자격증명을 발급할 수 있는 권한을 부여하는 기관을 의미한다.

ESSIF에서는 신뢰 등록 기관(Trusted Registration Authority)이 EBSI 원장을 작성할 수 있는 권한, 즉, DID를 원장에 쓸 수 있는 권한을 가지며, 신뢰 승인 기관(Trusted Accreditation Organization)은 신뢰 발급자에게 특정 유형의 검증가능한 자격증명을 발급할 수 있는 권한을 부여할 수 있는 권한을 가지는 기관이다.

ToIP에서 EGF의 관리 기관(Governing Authority)이 발급자에게 VC를 발급할 수 있는 유형에 대한 권한을 부여하고, 검증기관은 VC를 요청할 수 있는 유형에 대한 권한을 부여한다.

SGF에서는 소브린 스튜어드에 의해 운영되는 소브린 원장에 거래 작성자(Transaction Author)에게 쓰기, 기 등의 권한을 부여한다.

3.4.2 신뢰저장소

ESSIF에서는 신뢰 등록 기관 저장소, 신뢰 승인 기관 저장소, 신뢰 발급자 저장소 등의 저장소를 운영한다. 신뢰 승인기관 저장소는 도메인마다 존재할 수 있다.

ToIP에서 신뢰저장소는 각 EGF의 정부 기관(Governance Authority)에서 운영한다.

SGF에서 신뢰 발급자는 신뢰연결로 정의하고, SGF V2에서 정의한 정책에 따라 신뢰연결을 인증한다.

3.4.3 서비스 주체

서비스 주체는 DID 프레임워크에 참여하는 주체의 역할에 따른 구분을 의미하며, 각 DID 프레임워크의 발급자의 정의에 따라 차이가 발생한다.

ESSIF에서는 특정 유형의 VC를 발급할 수 있는 권한을 가지는 신뢰 발급자와 VC를 요청하는 검증기관 또는 신뢰 당사자가 있다.

ToIP에서는 특정 유형의 VC를 발급할 수 있는 발급자와 특정 유형의 VC를 요청할 수 있는 검증기관이 있다. 특히 검증기관의 경우 다른 프레임워크와는 다르게 관리기관을 통해 검증기관이 요청할 수 있는 VC의 유형을 승인받아야 한다.

3.4.4 기술 규격

각 DID 프레임워크에서는 기술규격을 크게 DID 식별자를 식별하고 검증하기 위한 암호학적 방법, VC를 생성하고 검증하는 방법 그리고 신뢰저장소의 정보를 기록하고 조회하는 방법을 제공한다. 이를 위하여 각 프레임워크는 W3C의 Decentralized Identifiers v1.0 규격[9]과 VC Data Model v1.1 규격[7]을 참조한다.

3.5 시사점

EU는 국경을 넘는 전자상거래 서비스를 구현하기 위해서 디지털 신분증 관련 정책을 마련하고, 규정에 부합하는 서비스를 개발하는 하향식(top-down) 정책을 수립했다. 또한, EU는 CEF 구성요소로 eID를 마련하면서 신분증 체계를 통일했다.

소버린 거버넌스 프레임워크는 글로벌하게 자기주권신원 모델 간 상호운용을 보장하기 위해 도메인 별 원칙 및 정책 정의했다. 이는 도메인 별 자기주권신원 도입 효과를 높이고, 도메인 별 고려사항을 반영할 수 있는 유연한 접근법이다. 추후 ToIP의 기본모델로 발전했다.

최근 W3C에서 URL 이후의 식별자로서 DID를 공식 표준으로 선정했다. 구글, 애플, 파이어폭스 등 기존 웹브라우저 시장을 선점하고 있던 플레이어들이 반대하였으나, 결론적으로 DID는 정식 표준으로 인정됐다[21]. 이는 디지털 시대에 부합되는 식별자로써 DID가 활용될 수 있는 가능성을 시사한다.

국내의 경우, 블록체인 시범사업을 통해서 서비스 개발이 선행되었으며, 서비스 간 상호운용이 부족하여 현재 표준화를 진행 중이다. 상향식(bottom-up) 접근으로 분야별로 서비스 모델을 마련하고 있으나 한계를 가지고 있다. 디지털 신분증을 아우를 수 있는 하향식 접근 및 관련 정책을 발굴해야 한다.

Ⅳ. 고려사항

4.1 정부의 역할

정부가 DID 생태계에 관여하는 것을 두고, 블록체인과 DID의 철학, 탈중앙화를 훼손한다는 의견이 있다. 어떤 중앙화된 주체나 신뢰할 수 있는 중개인 없이도 독립적으로 운영될 수 있어야 글로벌 확장성을

제공한다고 한다[22]. 확장성 측면에서는 동의하지만, 신뢰성 측면에서 재고해야 한다.

악의적인 공격자가 유령회사를 차리거나 기존의 기업으로 위조하여 신분증이나 증명서를 발행하고, 검증기업에 제출한다면 전자서명 검증과정에서 기술적 문제가 없으므로 이를 수용한다. 공격자는 디지털 신분증과 증명서의 정보를 악용할 수 있다. 더불어 최근 허위로 만든 증명서인지, 정부 기관에서 발급한 증명서인지 시스템이 걸러내지 못했던 사례도 존재한다[23].

DID 철학에 충실하면 글로벌 확장성을 갖추겠지만, 발행기관의 신뢰성을 서비스 제공기업이 보장해야 한다. 일반기업이 보장하는 증명서는 활용범위의 한계를 가진다. 정부의 과도한 시장 개입은 견제해야 하지만, DID 서비스에 대한 최소한의 신뢰성은 정부가 보장해야 한다. 이는 국가 간의 신분증, 증명서 검증을 위한 초석이다.

4.2 본인확인수단

공공과 민간 분야를 연계할 공통 식별자가 없다. 사용자는 국내 인터넷 서비스를 이용하기 위해서 회원가입을 하려면 문자인증, 금융인증, 카드인증 등을 통해서 본인확인 과정을 거쳐야 한다. 민간에서는 법적 근거없이 주민등록번호를 직접 수집하지 못하도록 했다. 주민등록번호는 개인정보보호법 제24조의2(주민등록번호 처리의 제한)에 의해서 일반기업이나 공공기관은 개인의 동의를 구했어도 수집할 수 없다[24].

이로 인해서, 민간에서 사용자를 식별하기 위해서는 주민등록번호를 해시 암호화한 88바이트의 식별 값인 연계정보(Connecting Information, CI)를 사용한다[25]. 이 연계정보는 한 기업이 다른 기업과 서비스와 연계를 위해 사용자를 식별할 때 활용한다.

국내는 해외보다 온라인 환경에서 사용자를 식별하는 수단이 발달했다. 공공·금융서비스 등 실지명의가 필요한 서비스를 이용하기 위해서는 지정된 본인확인기관에서 제공하는 주민등록번호 대체수단인 공동인증서, 휴대폰 본인확인, i-Pin 등을 활용한다. 이때 본인확인기관이 서비스 기업에 본인확인 목적으로만 CI를 제공함으로써 사용자를 식별한다.

DID는 신원확인부터 자격증명까지 활용할 수 있는 서비스이다. 특히 DID 기반의 인증 서비스는 주민등록번호 등 민감 정보를 플랫폼 사업자가 아닌 정보주체인 사용자 자신의 단말에 직접 보관했다가 제출한다. CI를 증명서에 내려받으면 국내의 대부분 민간서비스를 연계할 수 있지만, 이는 CI를 본인확인 목적 외로 재사용하게 되므로 취지에 어긋난다. 또한, 사용자 부주의로 CI정보가 노출될 경우의 주민등록번호를 바꾸거나 CI 생성 모듈을 변경해야 할 만큼 영향이 크다.

이러한 국내 현황을 고려하여 민간 기업이 DID 서비스를 운영한다면, 글로벌 확장성이 낮아진다. 이를 위해서는 새롭게 시장에 진입하는 신기술 사업자들이 공정한 환경에서 경쟁을 펼치는 정책방안이 마련되어야 한다.

4.3 디지털지갑 시장 형성

EU 집행위원회는 새로운 디지털ID 지갑 계획 발표했다[26]. 2030년까지 EU 시민의 80%가 디지털 지갑을 통해 공공서비스 접속, 증명서 발급 등 일상에서 사용할 수 있도록 디지털전환 정부 전략을 추진 중이다[27].

이는 공공-공공, 공공-민간, 온라인-오프라인 간 디지털 신분증과 증명서를 자유롭게 주고받을 수 있는 생태계를 사전에 확보할 의도이다[28]. 출생증명서 발급, 세금 신고, 대학 입학 신청, 처방전 보관, 성인 증명, 은행계좌 개설, 대출 신청, 자동차 렌트, 호텔 체크인 등의 서비스를 마련할 계획이다.

캐나다에서도 디지털 지갑 서비스가 퍼지고 있다[29]. 또한, 국내 주요 인터넷 포털기업, ICT 대기업, 블록체인 기업이 디지털 지갑을 개발하고 지갑 서비스 확장하기 위해 경쟁하고 있다.

이러한 디지털 지갑은 블록체인 플랫폼을 서로 연계하는 상호운용성을 확보하는 것보다 생태계 활성화 측면에서 유리하며 실현 가능성 또한 높다.

Ⅴ. 신뢰연결(Trust Anchor) 프레임워크 기본모델

5.1 승인기관 및 중계기관의 역할

승인기관은 정책적으로 중계기관의 지정·의무이행 점검·취소 등의 관리권한을 가진다. 이에 승인기관은 중계기관에게 [표 4]와 같이 중계기관인증서 VC를 발급하고 해당 정보를 공개한다. 또한, 중계기관인증서는 다양한 증명서의 정보와 결합하여 VP로 제출될 수 있다. 중계기관인증서는 중계기관이 제공하는 정보에 신뢰성을 부여하고, 신뢰저장소를 관리하고 운영할 수 있다는 권한을 입증한다.

중계기관은 공공, 민간을 비롯하여 의료, 예술 등의 여러 분야마다 등록할 수 있으며, 발행기관의 신뢰성을 보장하기 위한 목적을 가진다. 중계기관은 기존 PKI 기반 전자서명 또는 DID를 사용할 수 있도록 신뢰연결정보를 신뢰저장소에 등록하여 관리한다. 사용자가 어떠한 전자서명기술 기반의 신분증, 증명서를

표 4. 중계기관인증서(VC) 데이터 명세(예시)
Table 4. Verifiable Credential (VC) Data Specification (Example) of Intermediate Authority

클레임(Claims)	내용
Registration date	등록일
Registered organization	등록기관
Relay entity type	중계기관 유형(PKI, DID 등)
Relay entity assurance level	중계기관 보장 등급
Relay entity name	중계기관명
Relay entity status	중계기관 상태
Relay entity status effective	중계기관 상태 유효
Relay entity proofs	중계기관 검증정보
Relay entity address	주소
Service endpoint	홈페이지 주소
Verifiable data registry	신뢰저장소 접속 경로
Effective date	유효기일
Expire date	유효마감일
Contact	연락처

사용하여도 중계기관의 신뢰연결정보를 통해서 발행기관을 신뢰할 수 있다. 발행기관은 중계기관의 신뢰연결정보를 기반으로 사용자에게 VC를 발급함으로써 신뢰를 이어간다. 이를 위하여 중계기관에서 제공되는 정보는 항상 중계기관의 전자서명과 인증서가 포함되어야 한다. 중계기관에 대한 신뢰는 바로 승인기관이 발급한 중계기관 인증서에서 시작되기 때문에, 전자서명과 인증서가 포함되지 않은 중계기관의 정보는 신뢰할 수 없는 정보이다.

검증기관은 사용자가 제출한 VP의 발행기관을 검증하기 위해 중계기관 인증서 정보의 신뢰저장소에 접속하여 발행기관 정보를 검증한다. 다수의 발행기관에서 여러 전자서명을 활용하여 제출한 경우에도 각 발행기관이 속해있는 중계기관의 신뢰저장소에 접근하여 검증할 수 있다.

기존 PKI 시스템에 제안하는 신뢰연결 프레임워크 기본모델을 적용할 경우 [표 5]와 같은 기관들이 관련 역할을 수행할 수 있다.

표 5. 역할 별 수행기관(예시)
Table 5. Organizations in charge by role

역할	수행기관
승인기관	정부부처, 공공기관
중계기관	본인확인기관, 전자서명인증사업자
신뢰저장소	본인확인기관, 전자서명인증사업자
발행기관	DID 플랫폼 사업자
검증기관	DID 서비스 수요기업

5.2 전자서명인증업무 기반 기술 별 검증방법

중계기관이 제공하는 신뢰연결정보는 PKI, DID 등 검증하고자 하는 인증기술에 따라서 검증방법이 다르다.

5.2.1 PKI 기반 전자서명인증업무

중계기관이 전자서명인증업무에서 최상위인증서 또는 최상위인증서를 조회할 수 있는 접속 경로를 신뢰연결정보로써 제공한다. 사용자 인증서를 검증하고자 하는 사용자는 중계기관으로부터 수신한 신뢰연결의 최상위인증서를 제공받아 가입자 인증서를 검증하고 신뢰연결이 인정사업자임을 확인할 수 있다.

신뢰연결의 최상위인증서와 중계기관의 최상위인증서가 같은 경우에는 인증서 경로 검증만으로 신뢰연결이 인정사업자임을 확인할 수 있다.

5.2.2 DID 기반 전자서명인증업무

중계기관은 신뢰저장소 접속 경로를 신뢰연결정보로써 제공한다. 검증기관은 중계기관의 신뢰연결정보를 통해서 발행기관을 검증한다. 사용자 검증은 검증기관이 사용자의 DID를 발행기관이 속해있는 블록체인 네트워크에 전달해서 검증한다. DID의 검증정보가 저장되어 있는 DID 문서는 블록체인 네트워크에 항상 최신 상태로 유지해야 한다. 또한, 검증기관은 사용자의 DID를 검증하기 위해 직접 DID 문서를 확인할 수 있어야 한다.

중계기관은 하위 발행기관의 DID 리졸버 드라이버(resolver driver)를 보유하여 DID 서비스 간 상호운용이 가능하도록 구현해야 한다. DID 리졸버 드라이버는 DID에 대응하는 DID 문서를 생성, 읽기, 업데이트, 삭제 등의 기능을 구현한 모듈이다. 중계기관은 DID 서비스를 제공하는 리졸버 드라이버를 연계하여 유니버셜 리졸버를 운영할 수 있다. 이때, 어떤 DID 서비스를 이용하여도 중계기관의 유니버셜 리졸버를 통해서 다양한 DID 서비스 간 상호운용을 제공할 수 있다.

5.3 중계기관 신뢰저장소 제공기능

중계기관은 신뢰연결서비스를 효율적으로 제공하기 위하여 중계기관 신뢰저장소를 운영할 수 있다. 중계기관 신뢰저장소는 중계기관이 전자서명인증사업자, DID인증사업자에 대한 신원 및 법인 확인을 통해 검증된 정보를 관리하는 저장소이다. 신뢰연결서비스 이용을 원하는 사용자가 언제든지 접속할 수 있도록

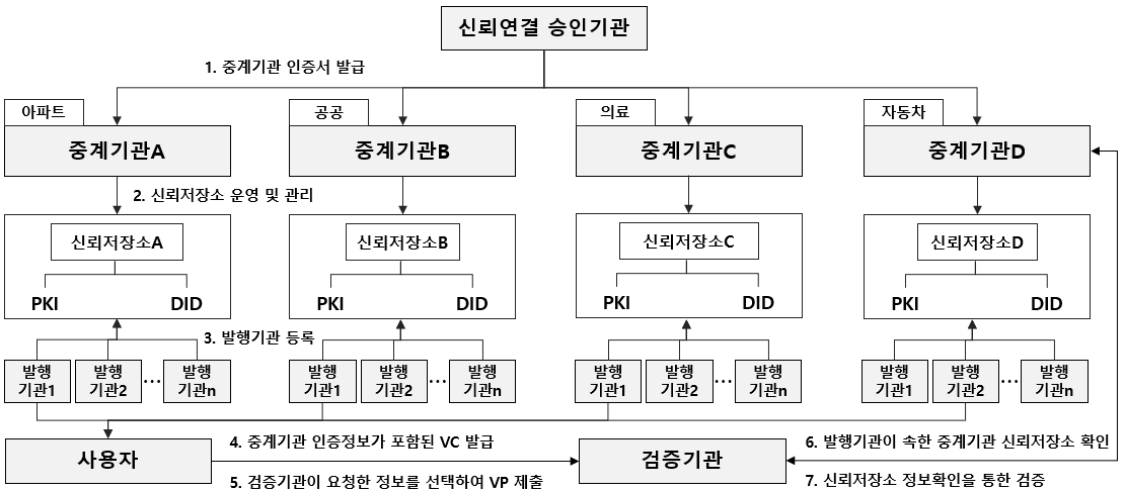


그림 6. 신뢰연결 프레임워크 기본모델
Fig. 6. Basic Model of Trust Anchor Framework

운영되어야 하며 다음의 기능을 제공할 수 있다.

- PKI 기반 전자서명인증사업자 조회 : 사용자는 중계기관의 신뢰저장소를 통해서 가입자 인증서의 발행기관에 해당하는 PKI 기반의 인정사업자 정보를 직접 조회
- DID 기반 전자서명인증사업자 조회 : 사용자 또는 검증기관은 VC, VP를 검증하기 위해서 중계기관에 해당 DID 발행기관의 전자서명 정보를 직접 조회 가능

5.4 공공-민간 분야 간 식별자 연계

공공분야의 중계기관은 서비스 제공 전 사용자로부터 최초에 DID 식별자 정보를 전달받는다. 이 식별자는 주민등록번호와 맵핑한다. 이후 해당 DID 식별자를 가지는 디지털 지갑에만 정부의 신분증, 증명서를 제공한다.

민간분야의 중계기관은 공공과 같은 방법으로 최초 서비스 이용시 CI와 DID 맵핑 데이터를 생성한다. 공공-민간 서비스 간 공통 식별자로 DID를 활용함으로써 분야와 관계없이 신분증, 증명서를 검증할 수 있다.

식별자 맵핑 데이터는 중요데이터로 분류하여 중계기관만이 관리하며 외부에서 확인할 수 없어야 한다.

5.5 신뢰연결 프레임워크 기본모델의 장단점

제안하는 모델은 전자서명인증과 DID 간 상호운용이 가능한 신뢰연결 프레임워크 기본모델로써 현재 신원확인 생태계를 보전하면서 DID를 적용할 수 있는 방안이다. 정부는 민간을 침해하지 않는 범위에서 최소한의 역할을 수행하면서, 분야별로 별도의 정책을 설정할 수 있다. 이로써 DID를 사람을 식별하기 위한 목적 이외에 사물 등에 도입하기 위한 기술적·정책적 유연성을 가진다.

하지만, 제안한 모델은 공공 및 민간 분야에서 사람을 특정할 수 있는 식별자로 주민등록번호, CI정보 등을 활용하는 국내 환경에서 효과적인 모델일 수 있으나 해외에는 걸림돌이 되는 구조이다. 해외는 DID를 식별자로써 활용하는 반면, 제안한 모델에서는 DID를 기존의 식별자에 접근하기 위한 목적으로 활용하는 단점을 가진다. 공공, 민간 분야에서 사람을 식별하는 식별체계가 다르다는 점을 유지해야 하는 한계를 가진다.

이에 향후 연구에서는 신뢰연결 프레임워크 기본모델을 토대로 글로벌 연계가 가능한 시나리오 및 정책 방안에 관해 연구하고자 한다.

Ⅵ. 결 론

본 논문은 공동인증서, 휴대폰 본인확인 등 본인확인서비스와 상호운용이 가능한 신뢰연결 프레임워크 기본모델을 제안함에 있어 의미를 가진다. DID 서비스 간 상호운용은 유니버셜 리졸버 및 DID 메소드 기능을 포함한 드라이버를 공유하는 방식으로 접근할 수 있다.

하지만, 중앙방식의 기존의 본인확인 서비스와 탈중앙방식 DID 연계에는 제약을 가진다. 또한, DID는 발행기관에 대한 별도의 신뢰체계를 마련해야 VC 발행의 신뢰성을 보장할 수 있다. 이는 정부에서 DID

및 기존 본인확인 서비스 간의 신뢰성을 보장하기 위한 최소한의 역할이 필요하며, 본 논문에서 그 범위를 신뢰연결 프레임워크 기본모델로 정의했다.

EU에서는 DID 기반의 신분증, 증명서 서비스를 마련하고 있으며, 글로벌 자동차 제조업체들은 PKI 기반의 운전면허증 표준을 마련하고 있다. 국내의 경우 사람에 대한 신원인증은 대부분 PKI 기반의 서비스이다.

사례로 자동차를 타고 집에 들어오기까지 자동차를 식별하고, 사람을 인증하고 자동으로 문이 열리고 가전기구가 동작되는 스마트홈을 구축하려면, 온라인-오프라인, 사람과 사물, 분야에 따라 다양한 전자서명을 활용할 수 있는 신원확인 또는 인증서비스가 필요하다.

제안하는 모델은 DID와 PKI 간 상호호환이 가능한 모델로 다양한 스마트 기기 및 서비스를 연결하고 인증하는데 기반이 될 것으로 기대한다.

References

[1] Personal Information Protection Commission, "*Annual Report on Personal Information Protection*," pp. 2-30, 2020.

[2] Gatner, "*Hype Cycle for Blockchain 2021; More Action than Hype*," Jul. 2021.

[3] Technavio, "*Blockchain Identity Management Market by End-user, Application, and Geography - Forecast and Analysis 2021-2025*," Jun. 2021.

[4] S. Nakamoto, "*Bitcoin: A Peer-to-Peer Electronic Cash System(2008)*," 2022.4.30. 1-11. from https://bitcoin.org/bitcoin.pdf (https://doi.org/10.2139/ssrn.3440802)

[5] G. Wood, "*Ethereum: A secure decentralised generalised transaction ledger(2022). Ethereum project yellow paper*," 2022.4.26. 1-41. from https://ethereum.github.io/yellowpaper/paper.pdf

[6] J. Lee, K. Lee, and K. Kwon, "Current status of blockchain-based decentralized ID ecosystem and policy suggestions," in *Proc. KICS Winter Conf. 2020.*, pp. 1048-1049, YongPyung Resort, Korea, Feb. 2020.

[7] W3C, "*Verifiable Credentials Data Model v1.1*," 2022.3.3. from https://www.w3.org/TR/vc-data-model/

[8] K. Lee, "*The need for DID-based mobile IDs for the post-corona era*," KISA Report, Nov. 2020.

[9] W3C, "*Decentralized Identifiers (DIDs) v1.0*," 2021.8.3. from https://www.w3.org/TR/did-core/

[10] Korea.kr, "*Driver's license stored in smartphone launches mobile ID era*," Jan. 2022. from https://www.korea.kr/news/policyNewsView.do?newsId=148898562

[11] Aju Business Daily, "*S. Korean cases will be referred to international workshop on electronic vaccine certificates*," Jul. 2021. from https://www.ajudaily.com/view/20210714112031535

[12] European Union, "*Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/ec*," 2014.

[13] European Commission, "*DIGITAL eID*," 2022.7.24. form https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eID

[14] European Commission, "*eSignautre, What are the levels (simple, advanced and qualified) of electronic signatures?*," 2022.7.25. from https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eSignature+FAQ

[15] European Commission, "*EBSI*," 2022.7.25. from https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home

[16] European Commission, "*European Blockchain Partnership*," 2022.7.25. from https://digital-strategy.ec.europa.eu/en/policies/blockchain-partnership

[17] CEF Digital, "*EBSI Architecture, explained*," 2022.4.30. from https://ec.europa.eu/digital-building-blocks/wikis/download/attachments/447687044/%28210610%29%28EBSI_Architecture_Explained%29%28v1.02%29.pdf?api=v2

[18] Daniel Du Seuil, "*European Self Sovereign identity framework*," 2022.4.30. from https://www.eesc.europa.eu/sites/default/files/files/1._panel_-_daniel_du_seuil.pdf

[19] ToIP Foundation, "*Introduction to Trust Over IP*," 2022.4.30. from https://trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0-2021-11-17.pdf
[20] Sovrin, "*Sovrin Governance Framework V2 Master Document V1*," 2022.4.30. from https://sovrin.org/wp-content/uploads/Sovrin-Governance-Framework-V2-Master-Document-V1.pdf
[21] R. Swick and T. Berners-Lee, "*Director's Decision on DID 1.0 Proposed Recommendation Formal Objections*," Jun. 2022. from https://www.w3.org/2022/06/DIDRecommendationDecision.html
[22] S. Park, S. Kim, and D. Han, et al., "*The Great Conversion of Wealth, Coin Wars*," Hans media, May 2021.
[23] SBS News, "*COOV vaccine certificates can be forged within 3 minutes*," 2021.05.03. from https://news.sbs.co.kr/news/endPage.do?news_id=N1006304656
[24] Korea Legislation Research Institute, "*PERSONAL INFORMATION PROTECTION ACT, Article 24-2 (Restriction on Management of Resident Registration Numbers)*," 2022.7.25. from https://elaw.klri.r e.kr/eng_service/lawView.do?hseq=32442&lang
[25] G. Jang and J. Lim, "*Technologies of Trust: Online Authentication and Data Access Control in Korea*," Carnegie, Aug. 2021.
[26] European Commission, "*European Digital Identity Architecture and Reference Framework – Outline*," Feb. 2022.
[27] European Commission, "*Europe's Digital Decade: digital targets for 2030*," Mar. 2021.
[28] European Parliament, "*Updating the European digital identity framework*," 2022.4.30. from https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698772/EPRS_BRI(2021)698772_EN.pdf
[29] PCTF, "*Pan-Canadian Trust Framework Digital Wallet*," 2022.7.25. from https://diacc.ca/pctf-digital-wallet/

이 강 효 (Kanghyo Lee)

2014년 2월 : 한양대학교 컴퓨터공학과 졸업
2016년 8월 : 한양대학교 컴퓨터공학과 석사
2021년 3월~현재 : 전남대학교 정보보안협동과정 박사과정
2017년 4월~현재 : 한국인터넷진흥원 근무
<관심분야> 블록체인, 클라우드, 엣지컴퓨팅, 정보보안
[ORCID:0000-0002-6587-5081]

박 소 현 (So-Hyeon Park)

2016년 2월 : 성신여자대학교 IT학부 졸업
2020년 3월~현재 : 전남대학교 정보보안협동과정 석박통합과정
2016년 11월~현재 : 한국인터넷진흥원 근무
<관심분야> 개인정보, 블록체인, 정보보안
[ORCID:0000-0002-4974-3310]

김 현 준 (Hyunjun Kim)

2016년 8월 : 서울과학기술대학교 전자IT미디어공학과 졸업
2018년 3월~현재 : 전남대학교 정보보안협동과정 석사과정
2016년 4월~현재 : 한국인터넷진흥원 근무
<관심분야> 통신공학, 정보보안, 블록체인, 개인정보
[ORCID:0000-0003-3051-7986]

하 태 균 (Tae Gyun Ha)

2001년 2월 : 인하대학교 수학과 졸업
2021년 9월~현재 : 전남대학교 정보보안협동과정 석사과정
2000년 12월~현재 : 한국인터넷진흥원 근무

<관심분야> 전자서명, 개인정보, 블록체인, 네트워크
[ORCID:0000-0003-1680-7143]

유 주 열 (Yoo Joo Yeol)

2005년 2월 : 세종대학교 정보통신공학과 졸업
2015년 8월 : 아주대학교 정보통신공학과 석사
2018년 2월 : 숭실대학교 IT정책경영학과 박사
2006년 12월~현재 : 한국인터넷진흥원 근무

<관심분야> 블록체인, 네트워크, 개인정보
[ORCID:0000-0002-6179-7987]

김 경 백 (Kyungbaek Kim)

1999년 2월 : 한국과학기술원 전기 및 전자공학과 졸업
2001년 2월 : 한국과학기술원 전기 및 전자공학과 석사
2007년 2월 : 한국과학기술원 전기 및 전자공학과 박사
2007년~2011년 : University of California Irvine, 박사 후 연구원
2012년~현재 : 전남대학교 전자컴퓨터공학부 교수

<관심분야> 분산시스템, 소프트웨어 정의 인프라스트럭처, 빅데이터 플랫폼, AI기반 CPS, 재난대응시스템, 정보보안, 블록체인
[ORCID:0000-0001-9985-3051]