정 보 보 호 학 회 지
제 34 권 제1호, 2024. 2

블록체인 기반 분산환경 상에서의 신원인증 기술동향

김 명 길*, 권 민 호*, 이 현 희*, 오 시 몬*, 김 요 한*

요 약

최근 분산형 신원확인 서비스에 대한 수요와 공급이 많아지면서, 다양한 산업에서 이를 적용하고자 하는 연구, 개발과 더불어 국제표준화를 기반으로 국가 단위의 프로젝트가 활발히 추진 중이다. 본 논문에서는 블록체인 기반 분산 환경 상에서의 신원인증 기술에 대한 소개와 법, 제도, 기술, 보안 등 다양한 측면에서 이를 분석하고 최근 기술 동향들을 소개한다.

Ⅰ. 서 론

4차 산업혁명과 함께, IT 시장이 활성화되고 디지털 서비스와 인프라가 더더욱 활발히 보급됨에 따라 인터넷 상에서의 개인정보 신원인증은 더이상 빠질 수 없는 국가 산업의 주요 핵심으로 자리잡고 있다.

현재까지의 디지털 상에서 신원인증 기술은 단순히 아이디, 패스워드를 활용한 회원가입과 로그인에서부터 소셜네트워크 서비스를 통한 SSO(Single Sign On) 기술 기반의 연합신원인증 모델까지 지속적으로 발전해왔다. 이는 서비스 사업자들이 개인정보에 대한 소유권을 제공하되 신원에 대한 정보는 중앙화된 데이터베이스에서 관리하는 방식으로 동작한다는 공통점을 가지고 있다. 이와 같은 구조 때문에 악의적인 공격자에 따라 대규모의 개인정보가 유출되는 등 큰 피해를 초래하는 보안위협이 발생하고 있으며, 대응 기술의 중요성이 부각되고 있다.

본 논문에서는 블록체인 기술을 기반으로 분산환경 상에서 DID(Decentralized Idnetity) 기술과, 이를 기반으로한 SSI(Self-Sovereign Identity) 신원인증 기술을 소개하며 이를 위한 다양한 국내외 표준화 활동 및 프레임워크 현황을 소개한다.

Ⅱ. 디지털 신원확인

2.1. 디지털 ID

디지털 ID는 온라인에서 개인을 식별하고 접근 권한을 부여하는데 사용되는 전자적인 신원을 의미한다. 디지털 ID는 개인이 온라인상에서 식별 가능한 개인과 관련된 디지털로 인증되고 저장된 특성의 모음이다. 이러

한 특성은 주로 나이, 생일, 지문을 비롯한 태생적 속성과, 건강기록, 신용정보 등의 축적된 속성, 그리고 주민/여권 번호 등의 부여된 속성의 세 가지 속성으로 분류된다. 이는 온라인상에서 믿을 수 있는 신원 확인을 가능케 하며, 보안과 접근 통제를 강화할 수 있다[1]. 디지털 신원의 수명주기는 신원을 수집하고 등록하는 단계부터 적절한 자격 증명 발급, 인증 인프라를 통한 활용, 그리고 신원 데이터를 최신 상태로 유지하는 일반적인 단계를 가진다.

한편 디지털 ID는 신원을 식별하고 검증하는 측면에서, 오프라인상에서 사용되는 아날로그 ID와 공통되는 특징을 지니고 있지만, 추가로 ID의 고유성 및 안전성, 실시간 업데이트, 원격 접근 및 사용을 보장한다. 따라서 아날로그 ID에서 디지털 ID로 전환하는 경우 온라인 서비스의 범위를 생활의 영역으로 확장하는데 사용할 수 있다. 또한, 기업 입장에서는 디지털 ID 관리 프레임워크를 구축함으로써 ID 관리 비용과 규제 요구를 대폭 줄여 기업이 운영 비용을 줄일 수 있으며 소비자 입장에서는 확장된 온라인 서비스를 통해 높은 품질의 경험을 제공받을 수 있다.

2.2. 디지털 신원확인

디지털 신원확인은 온라인에서 전자적 수단을 사용

* (주)스마트엠투엠 (책임연구원, myeongkil@smartm2m.co.kr; 선임연구원, alsgh458@smartm2m.co.kr; 선임연구원, hyeonhui@smartm2m.co.kr; 연구원, simon@smartm2m.co.kr; 연구원, yohan@smartm2m.co.kr)

하여 사람 또는 엔티티의 신원을 확인하고 설정하는 프로세스다. 이는 온라인 서비스의 안전성과 신뢰성을 확보하며, GDPR(General Data Protection Regulation) 및 마이데이터 산업과 같은 개인정보보호 트렌드와 함께 중요성이 증가하고 있다[2]. 디지털 신원확인은 인증과 인가의 두 가지 주요 단계로 구성된다.

인증 과정은 지식 기반, 이중 인증, 생체인증, 신분증 확인, 데이터베이스 인증, 라이브니스 탐지 등 다양한 방법을 사용하여 온라인상에서 사용자를 식별하는 과정이다. 인증이 성공적으로 완료된 이후 어떤 권한과 자격을 가지고 있는지 확인하고 리로스에 대한 액세스를 허가해주는 과정이 인가 과정이다.

〔그림 1〕 디지털 신원 인증/인가

2.3. 블록체인 기반 디지털 신원확인

현재 인터넷 서비스 상에서 주로 사용되는 디지털 신원확인 기술은 대부분 중앙집중형 ID 관리 모델에 기반한다. 그러나 중앙 집중형 모델의 경우 중앙서버에 모든 사용자의 신원정보를 관리하기 때문에 해킹에 대한 근본적인 해결이 어렵고, 많은 보안위협사례 발생으로 인해 개인정보보호 강화에 관한 관심이 증가하게되어 이를 해소할 수 있는 탈중앙화 신원증명 기술에 관한 관심과 수요가 증대되었다. 이러한 배경 속에 웹 표준을 개발하는 조직인 W3C(World Wide Web Consortium)의 데이터 탈중앙화 운동으로 인해 블록체인 기술을 통해 탈중앙화된 방식으로 신원데이터를 저장하고 증명할 수 있는 방법이 연구되었고 표준화를 위한 활동이 국제적으로 활발하게 진행되고 있다[3].

블록체인 디지털 신원확인은 흔히 DID로 불리며, 기존 중앙 집중식 시스템에 비해 여러 측면에서의 다양한 장단점이 존재한다. 기본적으로 데이터의 무결성 및 불변성이 보장되며, 투명성을 보장하여 참가자간의 신뢰성을 부여한다. 또한, 사용자가 자신의 데이터에 대한 통제권을 직접 가지기 때문에 개인정보 보호를 강화할 수 있다. 반면 사용자가 개인정보를 직접 관리해야한다는 측면에서는 분실에 대한 소실 우려가 있을 수 있다.

Ⅲ. 블록체인 기반 신원인증 기술

DID 기술은 일반적으로 개인정보를 사용자의 단말기에 저장하여, 개인정보 인증시 필요한 정보만 골라서 제출하도록 해주는 전자 신원증명 기술이다.

이렇듯 사용자가 직접 통제권을 디지털화된 개인신원지갑에 소유하는 특징을 통해서, 외부 서비스의 의존과 종속없이도 개인정보를 검증시켜주고 제공할 수 있는 SSI 모델을 지원할 수 있다.

3.1. DID 인증의 주요 특징

DID 인증은 크게 3가지 주요 특징(지속성, 휴대성, 개인정보보호)으로 나누어볼 수 있으며 아래와 같다[4].

지속성은 사용자가 외부 환경의 변화와 독립적으로 자신의 신원정보를 지속적으로 사용 가능하며 서비스 제공자가 서비스를 중단하더라도 신원정보의 유효성이 유지될 수 있다.

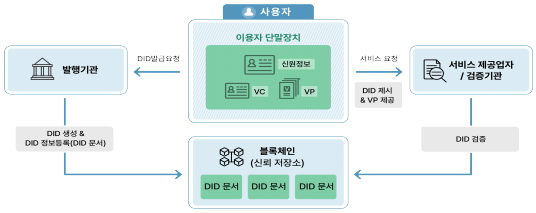
휴대성은 신원인증주체가 스마트폰이나 칩이 내장된 물리적 디바이스(카드 등)을 통해 신원정보를 저장하고 직접 이를 들고나디면서 쉽게 제공할 수 있다.

마지막으로 개인정보보호의 경우 사용자 동의 없이 서비스 제공자는 개인정보를 활용할 수 없다는 특징으로, 기존과는 다르게 신원정보를 사용자가 직접 스스로 관리하기 때문에 이를 조회할 수 있는 방법이 불가능하며, 절대적인 개인정보보호를 실현할 수 있다.

3.2. DID 시스템 구조

DID 기반 신원인증 서비스 과정은 SSI 모델을 기반으로 구성되며, 구조는 다음과 같다.

DID는 기본적으로 사용자의 요청에 따라 발행기관에 의해서 발급되며, 이는 신뢰할 수 있는 저장소인 블록체인 상에 검증가능하도록 기록된다. 사용자는 자신이 저장하고자하는 개인정보를 인증하고 발행 기관으로부터 검증가능한 인증서인 VC(Verifiable Credential)을 발급받아 자신의 단말에 저장할 수 있



〔그림 2〕 DID 기반 (신원인증) 서비스 구성도

다. 이후 발급된 VC를 통해 VP를 생성하여 서비스 제공자에게 제공함으로써 신원인증을 위한 요청절차가 마무리되며, 서비스 제공자는 신원인증 요청에 따라 블록체인 상에서 이를 검증하여 신원인증을 수행하고 리소스를 인가한다.

DID 시스템을 구성하는 참여자와 기본 구성 요소는 아래 표 1과 같다[5].

〔표 1〕 DID 시스템 참여자 및 기본 구성 요소

특징	설명
DID	신원을 가리키는 고유한 식별자
DID Document	인증에 사용되는 검증 정보
Verifiable Credential	검증 가능한 정보가 담겨있는 인증서
Claim	대상이 되는 신원(이름, 나이 등)
Issuer	신원을 확인하고 DID를 발급하는자
Holder	증명서를 보유하고 제시하는 자
Verifier	자격을 확인하는 주체
Resolver	블록체인, 전자서명을 통해 신원을 검증하는 도구(혹은 서버)
Wallet	증명서를 저장하는 애플리케이션
Distributed Ledger	신원증명의 검증 값을 관리하는 신뢰된 분산원장
DID Consortium	분산원장을 운영하고 표준·규격 등을 협의하는 기업·기관 협의체
DID Method Spec	사용하는 분산원장/신원증명 수단별로 세부 사항을 규정

Ⅳ. 국내외 DID 동향

국내외에서는 정부 주도의 DID 프로젝트부터 민간 기업의 독자적인 프로젝트 참여와 같은 다방면으로 진행되고 있으며, 이를 통한 개인의 프라이버시 보호와 데이터 주권을 강화하는 새로운 패러다임이 형성되고 있다. DID 기술이 발전하면서, 관련 법률체계 및 기술적 규격 확립이 향후 연구개발 과정에서 중요한 과제로 부상하고 있다.

4.1. 국내외 동향

국내 DID 동향은 모바일 공무원증, 운전면허증, 간편인증 서비스 등 공공서비스 활성화를 위해 블록체인을 도입하고 있다. 또한, 국내 기술 기업들은 DID 서비스 활성화를 위해 “DID 얼라이언스 코리아”와 같은 비영리재단을 설립하여 DID의 표준화와 상호호완 가능한 프레임워크의 개발을 위한 목표로 주도하고 있다.

국외에서는 DID 기술은 ‘14년 7월에 발표 된 유럽연합(EU)의 eIDAS(Electronic Identifiaction and Trust Services) 규정의 개정과 호주 정부의 Disital ID 프로젝트와 같이 주요 국가 및 국제기구의 정책 변화를 중심으로 진행되고 있다. 유럽연합의 eIDAS 규정은 유럽연합 내 국경 간 전자거래나 온라인 서비스 이용을 위한 신뢰 기반 마련이 주된 목적으로, 모든 회원국에 직접 적용되며 전자 서명뿐 아니라 디지털 신원의 넓은 영역을 다루고 있다. 주요내용은 전자식별수단(eID)와 신탁서비스(전자서명, 전자 송달서비스, 전자 인감 등)로 두 개의 파트로 구성된다. eIDAS 시행 이후, 유럽연합 내의 전자거래 규모는 크게 증가했으며, 관련 시장도 빠르게 성장하였으나, 제한적인 사용범위, 기술 및 거래 환경의 변화로 인한 실용성 이슈 등과 같은 한계점이 존재하였다. 따라서, 유럽연합은 기존 eIDAS 규정의 한계점을 검토하여 높은 안정성과 신뢰성을 지닌 전자신원 솔루션의 접근 환경을 지원하고, 유럽연합 내 전역 전자서명법 확대를 위하여 ‘21년 6월에 위원회가 eIDAS 2.0 규정 개정안을 제안하였으며, ‘30년까지 유럽연합 인구의 80%가 유럽연합 기관 및 기업과 상호작용할 수 있는 디지털 신분증 시

〔표 2〕 eIDAS 2.0 주요 변경사항

특징	eIDAS 1.0	eIDAS 2.0
규제 범위	국경 간 디지털 서비스 미포함	국경간 디지털 서비스를 포함
보안 및 개인정보	높은 수준의 보안 및 개인정보보 보호 제공	전자 신원 및 개인정보 보호 강화
디지털 신원	디지털 ID 생성 및 사용을 위한 프레임워크 미제공	EUDI 지갑 도입 및 사용가능한 프레임워크 구축
상호 운영성	국가 시스템 간 상호 운용성을 고려하지 않음	국가 시스템 간 상호 운용성 중점

스템을 보유할 것으로 예상하고 있다. eIDAS 2.0의 주요 변경사항으로는 신뢰 서비스의 확장과 EUDI 지갑 도입이 있다[6].

호주정부는 디지털 혁신처(Digital Transformation Agency, DTA)를 설립하고 디지털 ID 시스템 개발에 착수하였으며, '19년 호주 국세청 세무 관련 서비스에 디지털 ID를 처음으로 도입하였다. '23년 6월 호주 정부는 "Data and Digital Ministers Meeting"에서 ID 보안 및 보호를 강화하기 위해 신원정보 회복력을 위한 국가전략(National Strategy for Identify Resilience)을 발표하였으며, '23년 7월 호주 정부는 향후 12개월 이내에 면허증, 메디케어 및 신분확인 카드 등을 온라인으로 확인할 수 있는 디지털 ID를 시행할 것이라고 발표하였다[7].

4.2. W3C DIDs 표준

현재 블록체인 기반 디지털 신원확인 기법의 보안 가이드 및 표준화는 DID의 핵심 아키텍처, 데이터 모델, 보안 기법 및 고려사항이 명시되어 있는 월드 와이드 웹 컨소시엄(W3C)에서 발행한 Decentralized Identifier (DIDs) v1.0가 유일하다. W3C는 DIDs의 표준화와 촉진을 위한 중요한 역할을 맡고 있으며, 여러 부문에서 DIDs의 추가 개발과 광범위한 채택 및 구현을 주도하고 있다. 현행되는 DID의 기본적인 사양은 W3C DIDs의 기본 원칙을 따르도록 권장하고 있으며, 이 원칙은 개인과 조직이 신뢰하는 시스템을 사용하여 자체 식별자를 생성하고, 디지털 서명과 같은 암호화 증명을 통해 식별자에 대한 제어를 증명할 수 있다[8].

〔표 3〕 W3C 표준 DID 프라이버시 고려사항

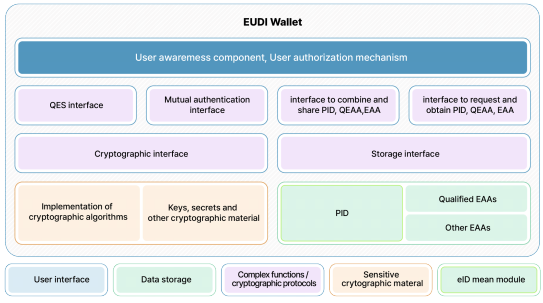
조항	설명
Keep Personal Data Private	DID 메서드 명세가 공개 데이터 레지스트리에 작성된 경우 DID 문서에는 개인정보가 포함되지 않아야 함
DID Correlation Risks	DIDs는 전 세계에서 중복되지 않는 식별자로 상관관계를 위해 사용 가능함
DID Document Correlation Risks	pairwise 식별자의 상관관계 보호가 제대로 작동하기 위해서는 DID 문서의 데이터도 서로 상관관계가 없도록 보장
DID Subject Classification	DID 문서에 DID주체의 유형이나 성질을 나타낼 수 있는 속성을 추가하는 것은 위험함
Herd Privacy	DID 주체가 다른 주체들과 구별되지 않는 경우 프라이버시가 강화됨
Service Privacy	한 DID 문서에 여러 서비스 엔드포인트를 사용하면 프라이버시 리스크가 발생할 수 있음

4.3. DID 프레임워크 현황

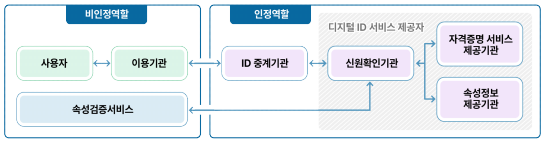
유럽연합 위원회는 '21년 6월경, 기존 프레임워크의 효율성을 개선하고 디지털 ID의 이점을 민간 부문과 모바일 활용으로 확대 전파함으로써 기존 단점을 해결하기 위한 목적으로 eIDAS 규정을 개정한 'EUDI를 위한 프레임워크 구축에 관한 규정안'을 공개하였다. EUDI 지갑은 각 회원국의 기존 국내 제도를 기반으로 구축되어 현행 eIDAS 규정에 따라 기존 eID는 계속 유효하나, EUDI 지갑을 통해 EUDI 기능과 사용성 확대가 가능하다. EUDI 지갑의 구조는 아래 그림 3과 같다[9].

EUDI 지갑으로 간편한 사용 및 정보 통제를 통해 시민들에게 편의성을 제공하고 있으며, 활용 가능한 분야로는 공공서비스(출생증명서, 의료증명서 등), 금융(은행 계좌 개설, 대출 신청 등), 세무(세금 신고서 제출), 교육(국내외 대학 지원), 기타(자동차 렌트, 주류 구매 등)와 같은 분야에 활용될 수 있다.

호주 연방 정부는 사용자 중심의 간단하게 접근이 가능하며, 디지털 신원을 제공하기 위한 TDIF 프레임워크(Trusted Digital Identity Framework)를 제정하였다. TDIF는 호주 전역 내 디지털 신원확인 서비스를 제공하는 서비스 제공자가 준수해야 하는 요구사항에 관한 규칙과 표준을 정의하고 있으며, 호주 정부 디지털 신원 시스템에 참여하는 모든 주체가 요건을 충족해야한다. 기존 디지털 ID 시스템은 시스템의 안정성 및 보안 우려로 인해 호주 정부, 주정부 및 준주 정부 등 다양한 기관이 참여하는 복잡한 구조를 가지고 있는 반면, TDIF는 역할을 인정사업자(Accredited



〔그림 3〕 EUDI 지갑 기능



〔그림 4〕 TDIF 참여기관 역할 구성

Provider)와 비인정사업자(Unaccredited Provider)로 구분하여 각각의 책임을 명확하게 정의하고 있다. 그림 4는 TDIF 참여기관의 역할 구성을 설명하고 있다[10].

Ⅴ. DID 보안 위협 분석 및 동향

5.1. 블록체인 기반 신원확인 서비스 분석

SSI 모델 기반의 신원확인 서비스는 DID 플랫폼 제공자가 DID 인증 서비스 의존 주체에 따라 서비스 참여 주체들의 “단말 앱 의존” 유형, DID “플랫폼 의존 유형”, 위 두 방식을 결합한 “하이브리드 의존 유형”으로 나눌 수 있다.

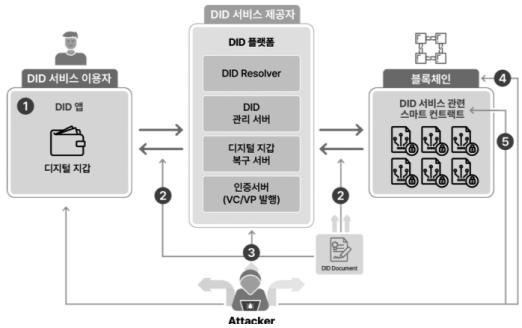
일반적으로 DID 서비스는 플랫폼 의존 형태로 구현되며, 해당 유형에서도 서비스 제공자의 선택에 따라 구성 요소가 달라진다. 크게 DID 디지털 지갑이 포함된 “DID 앱”, 서비스를 제공하는 “DID 플랫폼”, “블록체인(DID 문서 관리 레지스트리 및 DID 서비스 로직이 담긴 스마트 컨트랙트)” 부분으로 구분할 수 있다.

〔표 4〕 주요 블록체인 기반 신원확인 서비스 제공자

기업명		서비스명	유형
국외	마이크로소프트	Microsoft Security ID	플랫폼 의존형
	서버린 파운데이션	Sovrin	하이브리드형
	리넘랩스	uPort	단말 앱 의존형
	셀프키	SelfKey Identity Wallet	하이브리드형
	시빅	Civic 플랫폼	플랫폼 의존형
국내	파라메타	MyID	플랫폼 의존형
	씨피랩스	MYKEEPiN	플랫폼 의존형
	라온시큐어	OmniOne	플랫폼 의존형
	SK 텔레콤	Initial	플랫폼 의존형
	마크애니	AnyBlock DID	플랫폼 의존형

DID에서 고려할만한 보안 공격의 목적은 사용자 신원 도용 범죄를 위한 전자서명키 탈취, 개인정보 탈취, DID 서비스 이용 불가능 목표로한 서비스의 가용성 침해 3가지로 나눌 수 있다. 주요 유형인, 플랫폼 의존 유형에서 발생할 수 있는 보안위협의 발생 가능한 지점은[11] 아래 그림 5와 같이 구분할 수 있다.

DID 플랫폼 의존 유형에서 발생할 수 있는 보안위협은 표 6과 같이 블록체인 항목에 대한 보안 위협이 추가된 형태에서 일반적인 SaaS(Software as a service) 플랫폼 보안 위협과 크게 다르지 않다.



〔그림 5〕 DID 플랫폼 의존형 보안위협 발생 지점

〔표 5〕 주요 블록체인 기반 신원확인 서비스 제공자

객체	주체	환경	상세요소	설명
App	사용자	단말기기	디지털 지갑	개인정보, 인증서, 비밀키 등 신원정보를 관리
플랫폼	서비스 제공자	IDC/ 클라우드	DID Resolver	블록체인에서 DID를 해석하고 관리하는 서버
			DID 서버	DID 서비스를 제공
			지갑 복구	개인키 분실/훼손 복구
			VC/VP 발행 서버	사용자 VC/VP를 발행하는 서버
블록체인	블록체인 운영사	IDC/ 클라우드	스마트 컨트랙트	DID 서비스 로직을 수행하는 컨트랙트

〔표 6〕 구성 객체 별 보안 위협 발생 예시

발생 위치	상세 구분	보안 위협	예시
1번	사용자	사회 공학	피싱 이메일, SMS, 이메일, SNS, 검색엔진 등을 통한 카드정보, 이름, 생년, 연락처, 배송지, 주소, 이메일, 핸드폰 번호 노출

발생 위치	상세 구분	보안 위협	예시
	DID 앱	디지털 지갑 공격	소스코드 분석을 통한 취약점(하드코딩 PW, 암호화 키 등) 스캐닝/공격자가 습득한 기기에 포렌식 툴을 이용하여 관리자 권한 및 저장 정보 탈취
2번	네트워크 통신	중간자 공격	기기·서버및수신기(POS등)간트래픽분석,스니핑 등으로 인해 정보가 노출되거나 종단간 암호화가 되지 않은 데이터 탈취
3번	DID 관리 서버	SQL 인젝션	공격자가 사용자 입력에 SQL 쿼리를 주입하여 잠재적으로 데이터베이스 기록 조작
	지갑 복구 서버 ·인증서버	크리덴셜 임의 변경	접근권한을 가진 내부 직원에 의한 사용자의 크리덴셜 정보를 임의 변경
	DID Resolver	캐시된 DID 문서 조작	DID Resolver상의 캐시된 DID 정보를 조작하여, 인증 과정을 공격자가 원하는 방향으로 조작
4번	블록체인 노드	51% 공격	블록체인 네트워크상의 자체의사결정이 가능한 기준의 의사결정에 필요한 합의 리소스를 초과하여 확보한 뒤, 블록체인 트랜잭션 내역을 조작하여 이익을 얻는 해킹 공격
		DDoS	네트워크 부하 발생, 스팸 거래 생성하여 거짓 거래의 유효성 검사로 처리 시간이 늘려 부하를 발생시키는 방식
5번	스마트 컨트랙트	리엔터런시 공격	특정 트랜잭션이 처리되기 전에 다시 새로운 트랜잭션를 요청함으로써 이중 처리를 유도하는 공격 방법

5.2. 보안가이드/표준화 동향

SSI 기술의 발전을 위해ITU-T, ISO/WD, ISO/NP, ISO/PWI, ISO/TC 307, W3C 등 다양한 국제 표준화 기구들은 활발하게 기술 표준화 작업을 진행하고 있다.하지만, DID 보안 가이드/표준화는 “ITU-T SG17”, “W3C” “NIST”과 같은 일부 기구들을 제외하고는 표준화 작업이 활발하지 않은 걸로 보인다. 특히, ITU-T SG17 X.1403 권고안은 DID 시스템에서 분산 원장 기술(DLT) 활용 시 고려해야 할 보안 요소들을 아래 표 7과 같이 종합적으로 제시하고 있다[12].

NIST SP 800-63 가이드라인은 디지털 환경에서의 신원 관리, 인증 및 비밀번호 정책 등을 다루는 IAL, AAL, FAL 등 보증 레벨 개념을 도입하여 표준 및 가이드라인을 제시하고 있다[13].

〔표 7〕 SG17 분산 신원관리 보안 지침

항목	설명
분산 원장 기술 보안	분산 원장 기술은 신원 속성 및 신원 정보 교환을 위한 분산 신원 관리 시스템을 가능하게 하는 신뢰할 수 있는 인프라를 제공함 신원 데이터에 대한 위협을 완화하기 위해 필요한 통제 방안에 대한 지침 제공
신원 데이터 암호화	원장 외부에 저장된 신원 데이터는 기밀이며 개인적인것으로, 데이터를 암호화 할 수 있어야 함
백업	사용자 지갑에 대한 적절한 데이터 복구 및 복원 기술이 필요하며 또한 사용자는 자신의 데이터가 원장에 보호되고 백업되어 있음을 확신할 필요가 있음
키관리	키 체인에 대한 접근은 관리되고 감사 가능해야함 사용자가 지갑을 저장하고 복원할 수 있게 하는 서비스가 Decentralized Identity and Access Management에 의해 제공될 수 있어야함
보안 리스크 완화	분산 원장 기술은 사이버 보안 위험으로 부터 정보 및 통신 기술 시스템을 완화하는 능력을 갖추어야 함
투명성 향상	분산 원장 기술은 여러개의 별도 보안 계층을 가지고 있어 멜웨어가 작동하기 어려우며, 분산된 신원 시스템은 분산 원장 기술에서 발생하는 보안 위험을 상속 받음
통신 네트워크 영향	분산 구조는 통신 네트워크 차원의 문제를 야기할 수 있으며 이 경우 발생하는 신원 데이터에 미치는 영향 및 블록체인 충돌 처리방법, 신원 데이터에 대한 재해 복구 계획등을 고려해야함

〔표 8〕 SP 800-63 가이드 라인 내 보증 레벨

기법	설명
IAL (Identity Assurance Level)	개인의 신원을 확실히 결정하기 위한 신원 증명 프로세스의 견고성을 나타내는 보증레벨, 주로 신원 증명 오류의 가능성을 줄이기 위해 사용
AAL (Authenticator Assurance Level)	AL은 인증 과정 자체의 견고성과 특정 개인의 식별자와 인증자 간의 연결 강도를 나타내는 보증 레벨, 주로 다른 사람이 자신의 것이 아닌 자격 증명을 사용하는 것을 방지하는 데 사용
FAL (Federation Assurance Level)	페더레이션이 인증 및 속성 정보를 RP(Replying Party)에게 전달하는 데 사용하는 주장 프로토콜의 견고성을 나타내는 보증 레벨. 이는 주로 RP에게 전달되는 인증 및 속성 정보의 정확성 보장하는데 사용

Ⅵ. 결 론

본 논문에서는 블록체인 기반 분산환경 상에서의 신원인증 기술인 DID와 이를 통한 SSI 기술에 대해 소개하고, 표준화 및 프레임워크 현황에 대한 조사와 더불어, DID 기술에 대한 보안위협에 대해 정의하였다.

최근 모바일 운전면허증 등 신원인증지갑을 통해 개인정보에 대한 소유권 뿐만 아니라, 데이터 자체도 직접 지갑에 저장하고 관리할 수 있도록 DID 기반의 자기주권형 신원인증 서비스가 보급되고 있다.

이번 연구를 통해 DID 기술에 대한 여러 특징들을 도출하여, 전반적인 흐름과 방향성을 확인할 수 있었다.

특히 블록체인을 기반으로한 신원인증은 국내뿐 아니라, 국제적으로도 높은 관심을 보이며 다양한 측면에서 많은 투자와 프로젝트들이 수행됨에 따라 시장이 형성되고 수요가 급증하고 있는 것을 알 수 있었다.

이러한 시장 수요를 대응하기 위해서는 디지털 신원인증의 특성상 절대적으로 보안위협에 대한 대응이 0순위로, DID 산업을 활성화하면서 지속적으로 글로벌 경쟁력을 확보하여 시장을 선도하기 위해서는 보안위협을 대응할 수 있도록 기술력 강화는 필수적으로 보인다.

참 고 문 헌

[1] 서승현, 이수진, “생애주기형 분산ID 서비스 활성화 방안 연구”, KISA Insight, Dec 2021.

[2] 장항배, 유진호, “디지털 메가트렌드에 따른 정보보호의 역할 분석 연구”, KISA Insight, Dec 2022.

[3] W3C, “Decentralized Identifiers (DIDs) v1.0 publication history”, Standard history, 2022.

[4] 금융보안원, “분산ID 개념 및 해외 기술 개발동향”, 전자금융과 금융보안 제16호, 2019. 04.

[5] Manu Sporny, Dave Longley, Markus Sabadello, Drummond Reed, Orie Steele, Christopher Allen, “Decentralized Identifiers (DIDs)”, W3C, July 2022.

[6] European Commission, “eIDAS made easy”, Quickstart Guide, Mar 2021.

[7] 한국행정연구원, “KIPA 규제동향”, 2022 봄호 KIPA 규제동향, 2022.

[8] REED, Drummond, et al. “Decentralized identifiers (dids) v1.0 Draft Community Group Report”, 2020.

[9] European Commission, “European Digital Identity Architecture and Reference Framework – Outline”, Shaping Europe’s digital future, 2022.

[10] ZHAO, Shengshi, et al. “Submission: Australian Government Digital Identity Legislation Position Paper”, UNSW Law Research Paper, pp.21-86, 2021

[11] 이재성, 우성도, “디지털 지갑의 사이버보안 위협 및 보안 요구사항 분석” KISA Insight, Vol.06, 2022.

[12] ITU-T SG17, “Security guidelines for using DLT for decentralized identity management”, X.1403 (X.dlt-sec), Aug 2020

[13] NIST, “Digital Identity Guidelines”, SP 800-63, Aug 2020

〈저 자 소 개〉

김 명 길 (Myeongkil Kim)

정회원

2017년 2월 : 부산대학교 정보컴퓨터공학부 졸업

2019년 2월 : 부산대학교 일반대학원 전기전자컴퓨터공학과 석사

2019년 3월~현재 : (주)스마트엠투엠 책임

2020년 3월～현재 : 부산대학교 일반대학원 정보융합공학과 박사수료

<관심분야> 블록체인, 정보보호

권 민 호 (Minho Kwon)

2020년 2월 : 울산대학교 사회과학부 졸업/IT융합 복수 전공

2022년 2월 : 울산대학교 일반대학원 전기전자컴퓨터공학과 석사

2022년 3월~현재 : (주)스마트엠투엠 선임연구원

<관심분야> 블록체인, 클라우드

이 현 희 (Hyeonhui Lee)

2020년 2월 : 동서대학교 컴퓨터정보공학부 졸업
2019년 06월~2020년 10월 : 토탈소프트뱅크 재직
2023년 2월 : 부산대학교 일반대학원 컴퓨터공학과 석사
2022년 9월~현재 : (주)스마트엠투엠 선임
<관심분야> 블록체인, 정보보호

오 시 몬 (Simon Oh)

2019년 2월 : 동서대학교 컴퓨터정보공학부 졸업
2022년 09월~현재 : 부산대학교 일반대학원 컴퓨터공학과 석사과정
2024년 02월 ~현재 : ㈜스마트엠투엠 연구원
<관심분야> 블록체인, 정보보호

김 요 한 (Yohan Kim)

2022년 2월 : 부산대학교 전기컴퓨터공학부 졸업
2024년 2월 : 부산대학교 일반대학원 정보융합공학과 석사
2024년 2월~현재 : (주)스마트엠투엠 연구원
<관심분야> 블록체인, 정보보호