디지털 신원확인 및 전자서명 수단 활용화 동향

박근덕 ITU-T SG17 Q10 (신원 관리) 부의장, 서울외국어대학원대학교 AI블록체인연구소/국제교양학과 교수

1. 머리말

최근 개정된 전자서명법에 근거하여 공인인증서 제도가 폐지됨에 따라 민간 회사에서 발급하는 사설인증서가 기존의 공인인증서와 동등한 지위를 가지게 됐다. 이와 함께 신흥 기술인 블록체인 및 분산원장기술을 이용한 분산신원증명(DID, Decentralized Identity)이 공공 및 금융 서비스 분야에서 이용자 신원확인과 전자서명 수단으로 주목받고 있다.

본고에서는 ITU-T SG17, ISO/TC 307, 월드와이드 웹 컨소시엄(W3C, World Wide Web Consortium), 미국표준기술연구소(NIST, National Institute of Standards and Technology), TTA PG502, 분산신원증명 기술 및 표준화 포럼 등 국내외 표준화 기구와 단체에서 다루고 있는 신원 관리 분야 표준화 동향을 살펴보려 한다. 이어 분산신원증명, 사설인증서 등 공공 및 민간 분야에서 활용하고 있는 신원 관리 기술 동향에 대하여 설명하고, 맺음말에서는 신원확인 적용 분야의 다양성 지원, 신원확인 서비스 이용자 보호 및 편리성 제고를 위한 요구사항 등을 제안한다.

2. 신원 관리 분야 표준화 동향

2.1 ITU-T SG17

ITU-T SG17은 ITU-T SG17 Q10(Identity management architecture and mechanisms, 신원 관리 구조 및 메커니즘) 연구과제를 통해 ITU-T X.gpwd, ITU-T X.tec-idms 등을 신규 권고안으로 개발하고 있다. ITU-T SG17 Q14(Security aspects for Distributed Ledger Technologies, 분산원장기술 보안) 연구과제에서는 ITU-T X.dlt-sec 등을 신규 권고안으로 개발했다.

미국 Aetna사에서 제안한 ITU-T X.gpwd (Threat analysis and guidelines for securing password and password-less authentication solutions, 암호 및 비암호 인증 솔루션 보안을 위

한 위협 분석 및 지침)는 공유 비밀 형식 기반 인증 솔루션의 보안과 위협 분석을 표준화한다. 기존의 암호 시스템과 최신 비암호 솔루션에 대한 보안 위협, 이용자 및 계정 보호를 위한 지침과 모범 사례 등을 포함하며[1], 2020년 9월 ITU-T SG17 회의에서 신규 워크 아이템으로 채택됐다.

Aetna사에서 제안한 또 다른 권고안인 ITU-T X.tec-idms(Management and protection techniques for user data protection in distributed identity systems, 분산 신원 시스템에서 사용자 데이터 보호를 위한 관리 및 보호 기술)는 분산 신원 시스템에서 이용자 데이터와 관련된 식별자 보호 기술을 표준화한다. 분산원장기술을 활용하지 않는 분산 신원 시스템과 관련된 활용사례 및 위협 분석, 식별자 비연결성 및 비익명화 기법, 위협 완화를 위한 가이드라인 등을 포함하며[2], 2020년 9월 ITU-T SG17 회의에서 신규 워크 아이템으로 채택됐다.

ITU-T X.dlt-sec(Security guidelines for using DLT for decentralized identity management, 탈중앙화 신원 관리를 위해 분산원장기술을 사용하기 위한 보안 지침) 권고안도 Aetna사에서 제안했다. 신원 관리에서 분산원장기술 데이터를 사용하기 위한 통신 관련 개인정보 및 보안 고려 사항을 표준화하며 2017년 9월 ITU-T SG17 회의에서 신규 워크 아이템으로 채택됐다. 본 권고안은 탈중앙화 디지털 신원, 분산원장기술을 이용한 탈중앙화 신원, 분산 원장 보안 고려사항, 보안 위협 및 취약점 등을 포함하여 2020년 9월 ITU-T SG17 회의에서 신규 제정 표준 (ITU-T X.1403)으로 채택됐다[3].

2.2 ISO/TC 307

ISO/TC 307/WG 2(Blockchain and distributed ledger technologies - security, privacy and identity, 블록체인 및 분산원장기술 - 보안, 프라이버시 및 신원)가 주도하고 ISO/IEC JTC 1/SC 27/WG 5(Identity management and privacy technologies, 신원 관리 및 프라이버시 기술)가 참여하는 공동 작업반(JWG 4)은 ISO/TR 23249, ISO/TR 23644 등을 신규 표준안(기술보고서)으로 개발하고 있다.

이탈리아 주도로 개발 중인 ISO/TR 23249 (Overview of existing DLT systems for identity management, 신원 관리를 위한 기존의 분산원장 시스템 개요)는 개인, 조직, 사물(IoT 및 객체), 기능 및 프로세스 그리고 분산원장시스템 내부와 전체를 포함한 기타 실체의 신원 관리, 행위자와 그들의 상호 작용 및 공통 인터페이스에 대한 설명, 구조(Architecture), 기존 관련 표준 및 프레임워크 등을 포함하며, 2020년 11월 현재 표준 개발 초기 단계인 WD(Working draft) 단계에 있다[5].

스페인과 영국 주도로 개발 중인 ISO/TR 23644 (Overview of Trust Anchors for DLT-based Identity Management, 분산원장기술 기반 신원 관리를 위한 신뢰 앵커 개요)는 신원 관리를 위해 블록체인 및 분산원장기술을 활용하는 시스템에 대한 신뢰 앵커 사용과 관련된 개념 및 고려 사항을 표준화한다. 신뢰 앵커의 유형, 기존의 분산원장기술 기반 신원 관리 시스템을 위한 신뢰 앵커 등을 포함하며 2020년 11월 현재 표준 개발 초기 단계인 WD(Working draft) 단계에 있다[6].

2.3 월드 와이드 웹 컨소시엄

월드 와이드 웹 컨소시엄(W3C)의 탈중앙화 식별자 작업반(Decentralized Identifier Working Group)에서 미국 주도로 개발 중인

'Decentralized Identifiers v1.0(탈중앙화 식별자 버전1.0)'은 탈중앙화 식별자의 핵심 구조(Core architecture), 데이터 모델 및 표현을 표준화한다. 식별자, 데이터 모델, 핵심 속성(Core properties), 핵심 표현(Core presentations), 방법(Method), 보안 및 프라이버시 고려사항 등을 포함하며, 2020년 10월 현재 표준 개발 초기 단계인 WD(Working draft) 단계에 있다[7].

미국 탈중앙화 신원 재단(DIF, Decentralized Identity Foundation)이 주도하여 개발 중인 'Peer DID Method Specification(Blockchain-independent decentralized identifiers), 피어 탈중앙화 식별자 방법 사양서(블록체인에 독립적인 탈중앙화 식별자)'는 2020년 8월 현재 W3C 회원의 합의가 없는 비공식적인 내부 문서로서 핵심 특성(Core characteristics), DID 문서, 프로토콜(Protocols), 구현, 보안 및 프라이버시 고려사항 등을 포함한다[8]. Peer DID는 페어와이즈(Pairwise) DID 또는 엔-와이즈(N-wise) DID를 의미하는 것으로, 애니와이즈(Anywise) DID처럼 불특정 다수를 대상으로 하는 공용(Global public) 신원확인 목적이 아니므로 특정 개인 간 신원확인 및 프라이버시 보호에 유리한 측면이 있다.

2.4 미국표준기술연구소

미국표준기술연구소(NIST)가 개발한 'A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems(블록체인 신원 관리 시스템을 이해하기 위한 분류학적 접근)' 백서는 블록체인 신원 관리의 기초, 블록체인 신원 관리 시스템 분류, 보안 및 위험 관리, 추가적인 고려사항, 활용사례 등을 포함하며, 2020년 1월 발행됐다[9].

본 백서에서 주목할 만한 것은 이용자의 식별자(Identifier), 증명서(Credential) 및 개인키 등을 신뢰할 수 있는 제3자에게 수탁하는 '보관 및 위임(Custody and delegation)' 모델이다. 이러한 모델은 보관자(Custodian)가 이용자의 증명서 및 개인키 등을 보관함으로써 이용자의 통제와 합의에 따라 신뢰 당사자(예: 서비스 제공자)에게 신원증명을 대행할 수 있다. 또한 보관자는 이용자에게 개인키 복구 메커니즘을 제공할 수 있고, 이용자와 보관자, 서비스 제공자와 보관자 간 상호 인증된 통신 채널을 제공할 수 있다.

2.5 TTA PG502

한국정보통신기술협회(TTA)가 주관하는 정보통신표준화위원회의 '개인정보보호/ID관리, 블록체인 보안 그룹'(PG502)에서 금융보안원이 주도로 개발한 '분산ID를 활용한 신원관리 프레임워크'(과제번호: 2019-1110)가 채택됐다. 제1부 프레임워크 구성 및 모델(신원관리 프레임워크 및 구현 모델, 분산ID 유형 등을 포함), 제2부 신원증명 및 상호연동 방법(분산ID를 활용한 신원증명 특성 및 방법, 신원관리 상호연동 방법 및 요구사항, 분산형 키 관리 요구사항, 신원증명 절차별 인증 및 암호체계 등을 포함), 제3부 정보보호 요구사항(보안위협, 보안요구사항, 개인정보 보호 위협, 개인정보 보호 요구사항 등을 포함)으로 구성됐으며, 2020년 12월 정보통신단체표준으로 제정될 예정이다[10].

또한 서울외대 및 순천향대에서는 가상자산 사업자가 국경 간 가상자산 송금(이전) 시 송금인과 수취인의 신원을 확인할 수 있는 분산원장 기술 기반의 서비스 모델을 표준화하는 '분산원장기술 기반 가상자산 송금 이용자 신원확인 서

비스 모델'을 제안했다. 이 모델은 2020년 3월 TC5 회의에서 신규 표준과제(과제번호: 2020-0028)로 채택됐고 가상자산 관련 자금세탁방지를 위한 고객확인의무 및 개인정보 가명 처리 등 요구사항, 가상자산 이용자 신원확인 서비스 모델과 데이터 규격 등을 포함하여 2021년에 정보통신단체표준으로 제정될 예정이다[11].

2.6 분산신원증명 기술 및 표준화 포럼

과학기술정보통신부가 추진하는 '분산신원증명 기술 및 표준화 포럼'(위원장: 순천향대, 사무국: 한국인터넷진흥원)이 2020년 9월에 설립됐다. 본 포럼은 정책 분과, 기술 분과, 운영 분과 등 3개 분과로 구성됐다. 순천향대, 서울외대, 세종대, 광주대, 아주대, 숭실대, 충남대, 금융보안원, 금융결제원, 소프트웨어정책연구소, 국가보안연구소, 한국조폐공사, 한국전자통신연구원, 한국전자부품연구원, 한국정보통신기술협회, 이니셜DID연합, DID얼라이언스, 마이아이디얼라이언스, 마이키핀얼라이언스 등 학계·민간·공공 분야의 기술 및 표준 전문가가 포럼에 참여하여, 분산신원증명 관련 상호연동 방안 연구, 분산신원증명 관련 국내외 표준화 추진 및 협력방안 연구, 분산신원증명 생태계 활성화 관련 정책 연구, 분산신원증명 국내외 기술·서비스·정책 동향 분석 등을 수행한다.

정책 분과(위원장: 서울외대)에서는 'DID 집중육성을 위한 대정부 정책'을 제안하는 것을 목표로 DID 서비스 활성화를 위한 신규 비즈니스 모델 발굴, 이기종 플랫폼 간 정책적 상호연계 방안 마련, DID 관련 법·제도적 이슈 발굴 및 개선 방안 마련 등 주요 과제를 수행한다. 기술 분과(위원장: 세종대)에서는 'DID 용어 정의 포럼 표준' 및 'DID 기술 요구사항 포럼 표준' 제정을 목표로 DID 표준 제정을 위한 용어 정의 및 표준화 항목(목차) 마련, 이기종 플랫폼 간 기술적 상호연계 방안 마련, 라이프사이클에 따른 기술적 요구사항 표준화 추진 등 주요 과제를 수행한다. 마지막으로 운영 분과(위원장: 순천향대)에서는 '생태계 활성화를 위한 대내·외 환경 분석'을 목표로 국내외 DID 관련 동향 조사 및 분석, 국내 DID 생태계 현황 조사, 플랫폼 서비스 정책 마련 등 주요 과제를 수행한다.

3. 신원 관리 분야 기술 동향

3.1 분산신원증명

민간 분야에서는 이니셜DID연합, DID얼라이언스, 마이아이디얼라이언스, 마이키핀얼라이언스 등이 주축으로 W3C 표준을 준용하여 개발한 분산신원증명(DID, Decentralized Identity) 기술 및 플랫폼을 개발해 출시했다. 공공 및 금융 서비스 제공 시 법 규정에 근거하여 필수적인 이용자 신원확인 분야에 국한되어 활용되고 있다.

공공 분야에서는 모바일 신원 인증 서비스인 '블록체인 통합 서비스 비패스(B PASS)'가 부산 블록체인 특구 사업으로 추진되고 있다. 비패스는 가족사랑카드, 부산시청사 방문증, 도서관 회원증 등에 활용할 예정이다. 행정안전부는 2020년 말까지 블록체인 기반 신분증 서비스 구축을 완료하고, 우선 정부세종청사 공무원 약 1만 명을 대상으로 모바일 공무원증을 발급하여 사용할 계획이다. 금융결제원은 블록체인 기반 신원인증 서비스인 뱅크사인(Bank Sign)을 통해 금융 서비스 제공을 위한 대면 및 비대면 고객확인 절차에 적용할 예정이다. 전 직원을 대상으로 하는 분산신원증명 기반 모바일 사원증을 도입하여 사무실 출입, 업무 시스템 및 교육 시스템

접속 등에도 활용하고 있다.

3.2 사설인증서

사설인증서는 공개키 기반구조(PKI, Public Key Infrastructure) 및 국제 표준(ITU-T X.509[4])을 준수하므로 기존의 공인인증서와 기술적인 차이점이 없다. 최근 개정된 전자서명법에 근거하여 공인인증서 제도가 폐지됨에 따라 민간 기업에서 발급하는 사설인증서를 이용한 본인확인 및 전자서명이 증가하고 있는 추세다. 통신 사업자, 인터넷 포털(Portal) 사업자, 금융 회사 등이 주도하고 있는 사설인증서는 공공서비스(연말정산간소화, 국민신문고, 정부24 등), 금융 서비스, 전자 상거래 분야에서 광범위하게 활용될 수 있어, 신원 인증 시장에서 분산신원증명(DID, Decentralized Identity)과 치열하게 경쟁할 것으로 예상된다.

4. 맺음말

분산신원증명은 사설인증서와 달리 탈중앙화 분산원장기술을 적용했다. 따라서 이용자가 자기 통제 하에 본인확인, 자격인증, 단순인증 등이 필요한 경우 선택적인 신원 정보 제공이 가능하다는 것이 장점이다. 이에 공공 및 금융 서비스 등 법 규정에 근거한 이용자 신원확인 분야에만 한정적으로 활용할 것이 아니라, 개인 간 신원확인, 사물 간 신원확인 등 다양한 분야에 활용될 수 있도록 아키텍처(Architecture)와 프레임워크(Framework)를 개발하고 적합한 비즈니스 모델(Business model)을 구축하는 한편, 국내외 표준화를 적극적으로 추진할 필요가 있다.

마지막으로 포스트 코로나 시대를 맞아 비대면 신원확인의 필요성이 강하게 대두되고 있다. 여기에 분산신원증명, 사설인증서 등 신원확인 및 전자서명 수단의 이용을 활성화하려면 이용자의 디지털 신원 도용 등 보안 사고를 예방할 수 있는 기술 및 서비스 모델을 개발해야 한다. 또한 신원 증명서 (재)발급 및 이용 시 절차를 간소화함으로써 이용자 편의성을 높이는 것이 시급하다. 신원 관리 사업자는 본인확인기관과 연계한 개인정보 처리 최소화, 전자서명인증사업자 인증(근거: 전자서명법), 정보보호 및 개인정보보호 관리체계(ISMS-P, Personal information & Information Security Management System) 인증(근거: 정보통신망 이용촉진 및 정보보호에 관한 법률, 개인정보보호법) 등을 통해 신뢰를 쌓아나가야 한다.

※ 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 지원에 의하여 수행됨 [과제명: 차세대 ICT 환경에서의 보안 및 개인정보보호 기술 국제 표준화 추진, 과제번호: 2019-0-00660]

주요 용어 풀이

- ITU-T SG17: 국제전기통신연합에서 '보안' 분야 표준을 개발하는 연구반
- ISO/TC 307: 국제표준화기구에서 '블록체인 및 분산원장기술' 분야 표준을 개발하는 기술위원회
- TTA PG502: 한국정보통신기술협회 산하 정보통신표준화위원회에서 '개인정보보호/ID관리, 블록체인 보안' 분야 표준을 개발하는 프로젝트 그룹
- W3C: 월드 와이드 웹 브라우저 / 서버 기술의 표준을 개발하는 교육·연구 기관 및 관련 회사의 단체

참고문헌

[1] ITU-T SG17, ITU-T X.gpwd: Threat analysis and guidelines for securing password and password-less authentication solutions, 2020년 9월

[2] ITU-T SG17, ITU-T X.tec-idms: Management and protection techniques for user data protection in distributed identity systems, 2020년 9월

[3] ITU-T SG17, ITU-T X.1403 (X.dlt-sec): Security guidelines for using DLT for decentralized identity management, 2020년 9월

[4] ITU-T SG17, ITU-T X.509 (Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks), 2019년 10월

[5] ISO/TC 307, ISO/TR 23249: Overview of existing DLT systems for identity management, 2020년 11월

[6] ISO/TC 307, ISO/TR 23644: Overview of Trust Anchors for DLT-based Identity Management, 2020년 11월

[7] W3C, Decentralized Identifiers (DIDs) v1.0 (Core architecture, data model, and representations), https://www.w3.org/TR/did-core/, 2020년 10월

[8] W3C, Peer DID Method Specification (blockchain-independent decentralized identifiers), https://identity.foundation/peer-did-method-spec/, 2020년 8월

[9] NIST, A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems, 2020년 1월

[10] TTA PG502, '분산ID를 활용한 신원관리 프레임워크' (과제번호: 2019-1110), 2020년 11월

[11] TTA PG502, '분산원장기술 기반 가상자산 송금 이용자 신원확인 서비스 모델' (과제번호: 2020-0028), 2020년 11월