이용자 보호 및 편리성 제고를 위한 신원 관리 서비스 모델

박근덕
개인정보보호/ID관리, 블록체인 보안 프로젝트그룹(PG502) 특별위원
서울외국어대학원대학교 AI블록체인연구소/국제교양학과 교수

1. 머리말

최근 공인인증서 제도 폐지로 모든 전자서명 수단에 동일한 효력을 부여하게 됐다. 이에 따라 생체인증과 블록체인을 포함해 다양한 전자서명수단(예: 분산신원증명서, 공동인증서, 사설인증서 등)을 이용하는 추세다. 또한 금융 분야에서는 특정금융정보법 개정으로 가상자산사업자(예: 암호화폐 거래소, 암호화폐 보관 사업자, 암호화폐 전자지갑 사업자 등)에게 자금세탁방지 의무(의심 거래 보고, 고액 현금거래 보고, 고객 확인의무, 전신송금 시 정보제공 등)를 부과했다. 이에 가상자산사업자는 이용자의 신원 정보를 수집하고 보관하며, 일정 금액 이상의 가상자산 거래 시 금융 당국에 보고해야 하는 식으로 비대면 시대 새로운 비즈니스 모델에서도 디지털 ID의 활용도는 증가하고 있다.

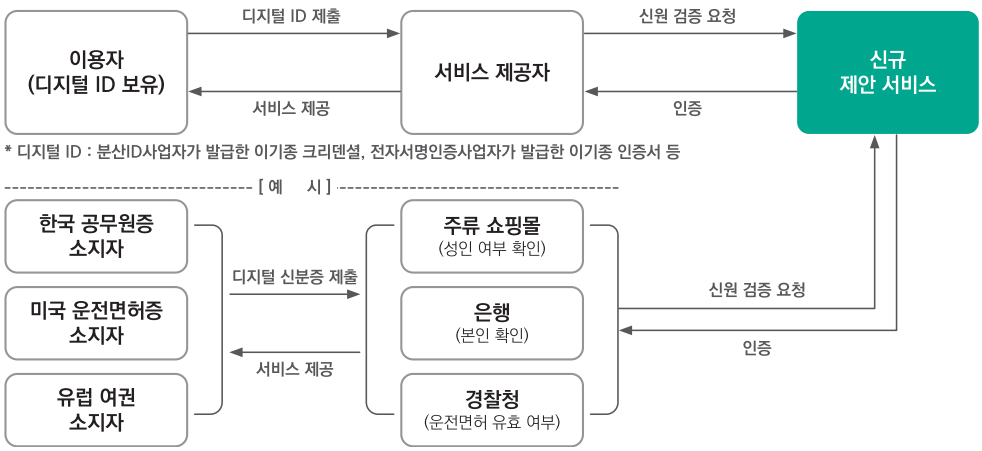
본고에서는 다양한 신원 인증 서비스 환경에서 이용자의 디지털 신원 정보 유출 및 사업자 간 ID 호환성 부족 같은 한계점을 해결하는 서비스 모델을 제안하고자 한다. 이는 이용자 단말기 해킹이나 분실, 도난에 의한 신원 도용 방지, 이기종 신원 관리 플랫폼 환경에서 이용자의 신원증명 절차 간소화(이용자 ID 발급 간소화: 1인 1ID 지향)를 달성하는 '디지털 ID 보관 및 연계 서비스 모델'이다.

2. 디지털 ID 보관 및 연계 서비스 모델

2.1 고려 사항

'디지털 ID 보관 및 연계 서비스 모델'은 다양한 신원 인증 서비스 환경에서 이용자의 디지털 신원 도용을 방지하고 이기종 신원 관리 플랫폼 환경에서 신원증명 절차를 간소화 할 수 있다. 이를 위해 다음과 같은 사항을 고려해야 한다.

- 신원 도용 방지처럼 이용자의 디지털 신원 보호를 강화하는가?
- 비정상적인 신원 증명 시도를 탐지할 수 있는가?
- 서비스별 ID 중복 발급, 앱(Application) 중복 설치같은 이용자 불편함을 해결하는가?
- 이용자가 본인의 신원 인증 이력을 모니터링할 수 있는가?
- 이용자 및 서비스 제공자에게 공개하는 API가 표준 프로토콜인가?
- 특정 신원 인증 플랫폼에 종속되지 않고 독립적으로 운영되는가?
- 도메인 간에 이용자 ID 연계 시 분산원장기술을 적용하는가?
- 공개키 인증서(공동인증서, 사설인증서 등)를 수용할 수 있는가?(확장성)



[그림 1] 이용자, 서비스 제공자, 신규 제안 서비스 간의 관계

- 국내외 표준에 근거한 정보보호 요구사항을 준수하는가?(ISMS)
- 국내외 법규에 근거한 개인정보보호 요구사항을 준수하는가?(개보법, GDPR)

2.2 제안 목적

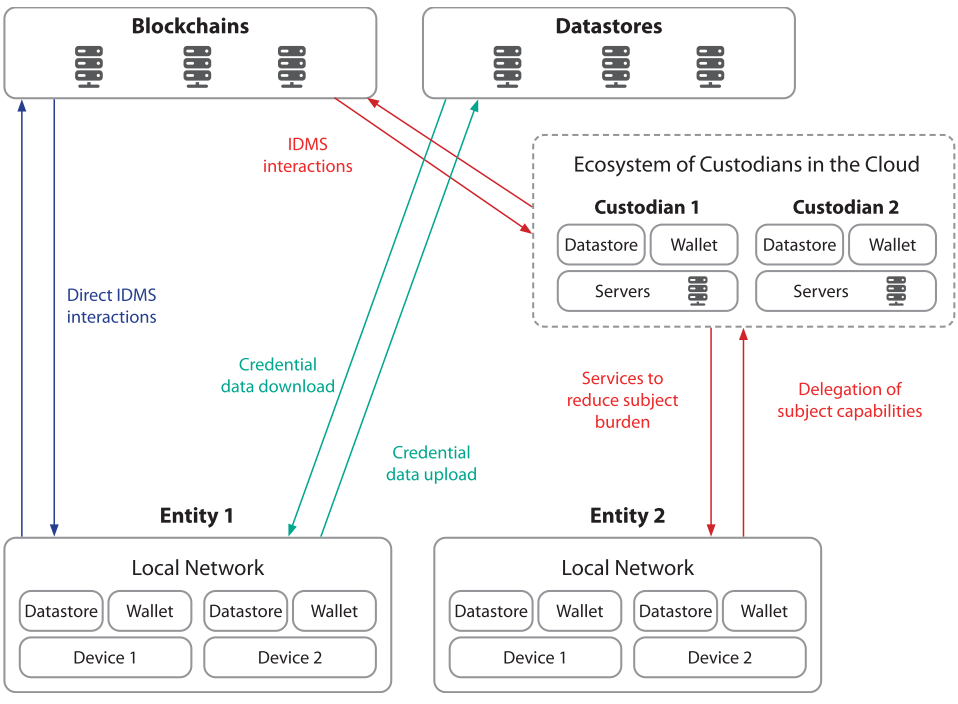
[그림 1]에서 보는 바와 같이 이용자가 제출한 디지털 ID의 발급자 및 종류에 관계없이 서비스 제공자는 이용자의 신원을 검증하고 그 결과(예: 본인확인, 자격인증, 단순인증 등)에 부합하는 서비스를 제공해야 한다.

'디지털 ID 보관 및 연계 서비스 모델'은 이용자의 ID 및 개인키를 안전하게 저장 및 관리함으로써 이용자의 디지털 신원 정보 보호를 강화한다. 또한 이기종의 신원 인증 서비스(예: 분산신원증명서, 공동인증서, 사설인증서 등)와 연동된 통합 ID(F-ID, Federation-ID)를 발급 및 공유하여 이용자 신원을 증명하는 것이 편리하다.

2.3 해외 사례

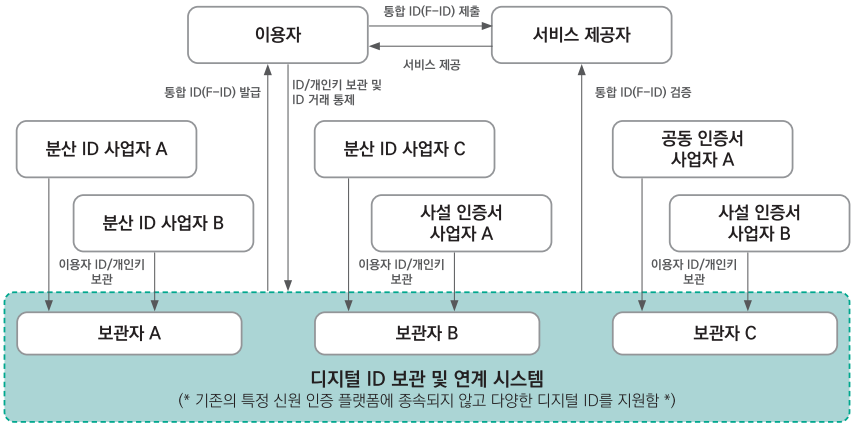
2020년 1월 미국표준기술연구소(NIST, National Institute for Standards and Technology)에서 발행한 '신흥 블록체인 신원 관리 시스템을 이해하기 위한 분류학적 접근방식(A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems)' 백서는 '식별자 및 증명서 관리 - 보관 및 위임(Identifiers and Credentials Management - Custody and Delegation)'에 대한 내용을 다룬다.

[그림 2]에서 보는 바와 같이 보관자(Custodian)는 실체(Entity)에게 정보주체(Subject)의 개인키 및 증명서 관리에서 생기는 부담을 덜어줄 수 있는 서비스를 제공한다. 실체는 보관자에게 정보주체의 능력(Capability)을 위임한다. 또한 보관

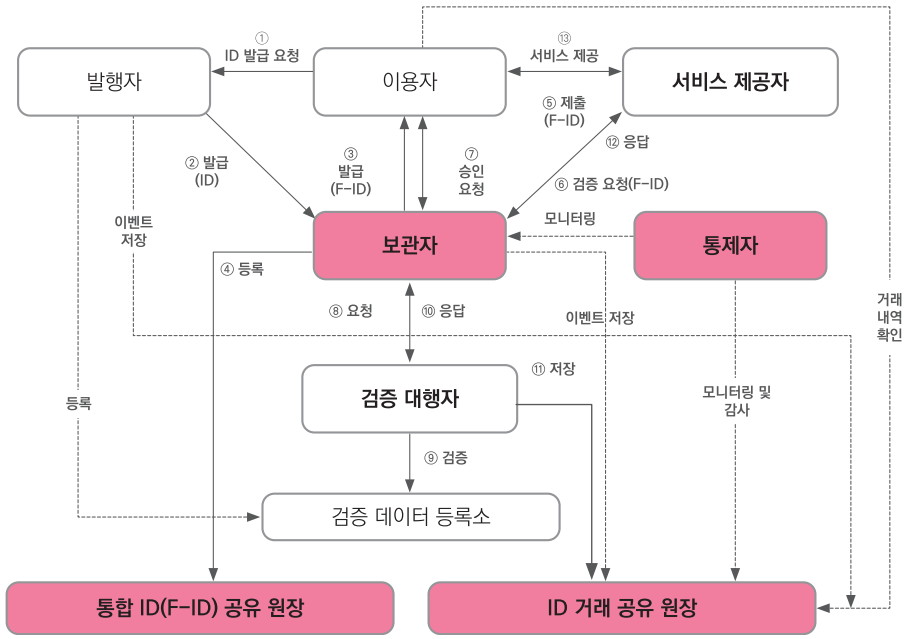


출처: NIST

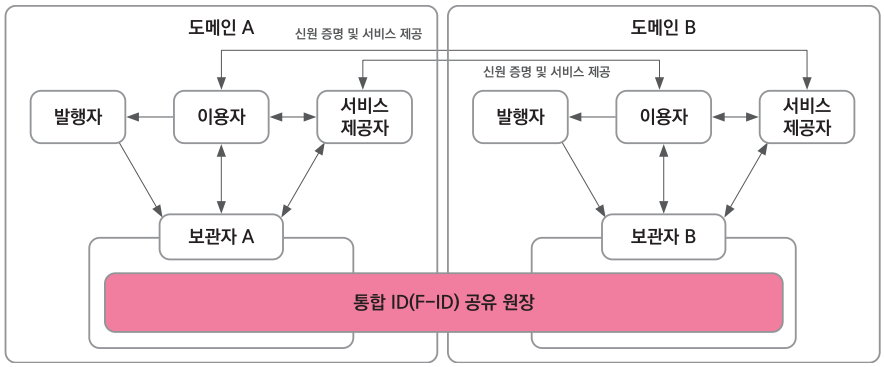
[그림 2] Interactions Between Subjects, Custodians, and Blockchains



[그림 3] 디지털 ID 통합 플랫폼 아키텍처



[그림 4] 디지털 ID 보관 및 연계 서비스 아키텍처



[그림 5] 통합 ID 연계 서비스 아키텍처

자는 블록체인을 활용해 신원 정보를 관리한다.

2.4 디지털 ID 보관 연계 서비스 모델 제안

이용자는 신원관리사업자(예: 분산ID사업자, 공동인증서사업자, 사설인증서사업자 등)에게서 발급받은 ID와 연동되는 통합 ID(F-ID, Federation-ID)를 활용해 서비스 제공자에게 본인의 신원을 증명한다.

[그림 3]에서 보는 바와 같이 신원관리사업자(예: 분산ID사업자, 공동인증서사업자, 사설인증서사업자 등) 등은 이용자의 ID 및 개인키를 보관자에게 위탁하고 보관자는 위탁받은 ID 및 개인키와 대응되는 통합 ID(F-ID)를 이용자에게 발급한다. 이용자는 서비스 제공자에게 F-ID를 제출해 신원 증명을 요청하고 서비스 제공자는 F-ID를 보관자에게 제출해 이용자의 신원 검증을 요청한다. 이를 통해 보관자끼리 F-ID를 공유해 도메인이 서로 다른 이용자와 서비스 제공자 간의 신원 증명이 가능하고, 보관자는 비정상적인 신원 검증 요청을 탐지해 이용자의 신원이 도용되는 것을 방지할 수 있다.

이용자는 발행자가 발급한 ID 및 개인키를 보관자에게 위탁하고, 보관자가 발급한 표준화된 F-ID를 사용해 본인의 신원을 증명한다.

[그림 4]에서 보는 바와 같이 'F-ID 공유 원장'과 'ID 거래 공유 원장'은 데이터의 위·변조를 방지하고 이해당사자들이 안전하게 공유하기 위해 분산원장기술을 적용한다. F-ID 공유 원장에는 이용자의 F-ID를 저장하고, ID 거래 공유 원장에는 이용자의 신원 인증 이력을 저장한다.

[그림 5]에서 보는 바와 같이 이용자는 보관자가 발급하고 공유한 표준화된 F-ID를 사용해 보관자별로 분리된 도메인에 관계없이 서비스 제공자에게 본인의 신원을 증명한다. 이는 상호 연동된 이기종의 신원 인증 시스템 환경에서 이뤄진다.

3. 맺음말

지금까지 분산신원증명서, 공동인증서, 사설인증서 등 다양한 이기종 신원 인증 서비스 환경에서 이용자의 디지털 신원을 보호하고 이용 편리성을 제고할 수 있는 '디지털 ID 보관 및 연계 서비스 모델'을 제안했다. 본 제안 서비스 모델은 이용자의 개인키 및 증명서 같은 신원 정보를 신뢰할 수 있는 보관자에게 위탁해 관리한다. 또한 이용자의 권한을 보관자에게 위임하고 통제해 신원 도용을 방지하고 신원 증명 절차를 간소화한다.

마지막으로 제안 서비스 모델은 이용자의 개인키만 보관자에게 위탁하는 모델, 이용자의 개인키 및 신원 증명서(Credential)를 보관자에게 위탁하는 모델, 통합 ID 공유원장 및 ID 거래 공유원장을 온-체 인(ON-CHAIN)에 저장하고 관리하는 모델(DLT 기반), 통합 ID 공유원장 및 ID 거래 공유원장을 오프-체인(OFF-CHAIN)에 저장하고 관리하는 모델(Non-DLT 기반) 등 4가지 유형으로 구분돼 국내외 표준화가 추진될 예정이다.

※ 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

- NIST: 미국 상무부 기술관리국 산하의 각종 표준과 관련된 기술을 담당하는 연구소
- TTA PG502: 한국정보통신기술협회 산하 정보통신표준화위원회에서 '개인정보보호/ID관리, 블록체인 보안' 분야 표준을 개발하는 프로젝트 그룹

참고문헌

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

[2] ITU-T SG17, ITU-T X.1252rev(Baseline identity management terms and definitions), 2020년 12월

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

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

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

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

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