탈중앙화 신원관리 서비스 모델

박근덕 서울외대 국제교양학과/AI블록체인연구소 교수, ITU-T SG17 Q10 부 라포처

1. 머리말

탈중앙화 신원관리 시스템은 이용자 중심의 신원관리 시스템으로, 발행자(issuer)와 소유자(정보주체, holder), 서비스 제공자(신뢰 당사자, relying party), 검증자(verifier), 데이터 저장소 등으로 구성된다. 분산원장기술(DLT, Distributed Ledger Technology)을 이용한 탈중앙화 신원관리 시스템은 DLT 시스템(블록체인)에 저장된 데이터의 무결성을 유지하고 DLT 시스템의 노드로서 참여자 간에 데이터를 투명하게 공유할 수 있는 장점이 있다.

소유자는 공개 및 개인 키 쌍과 함께 증명서를 저장하는 신원 지갑을 스마트폰 등 자신의 단말기에 설치하고 이용한다. 소유자의 개인 키는 서비스 제공자에게 제출하는 증명서의 전자서명에 사용된다. 소유자는 증명서의 보증 수준에 따라 개인키를 안전하게 보관하여 신원이 무단 도용되지 않도록 해야 한다. 이러한 탈중앙화 신원관리 환경에서 소유자는 개인키와 개인정보를 포함하고 있는 증명서를 스스로 안전하게 저장 및 관리해야 하는 부담을 지게 된다.

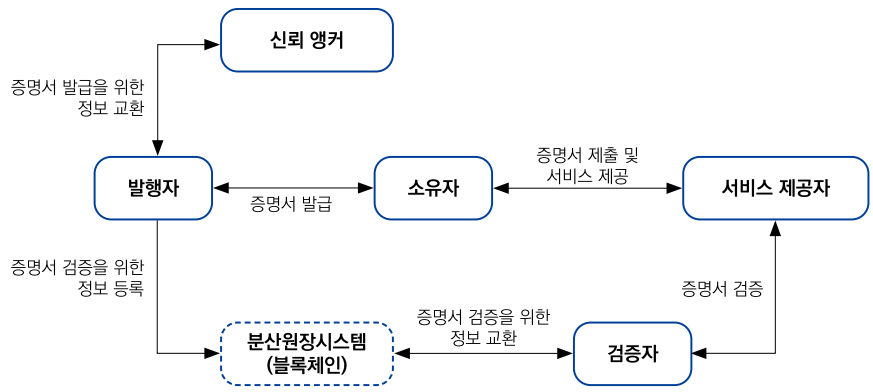
어떤 경우에는 소유자가 개인정보를 포함한 필수 정보를 제공하여 증명서를 직접 발행할 수 있다. 이러한 탈중앙화 신원관리 시스템에는 제3의 발행자가 필요하지 않다. 즉, 소유자는 발행자이기 때문에 디지털 명함, 출석 증명서, 여행 방문자 증명서, 음식 및 음료(F&B) 주문 증명서 등을 직접 발행할 수 있다.

최근 국내외적으로 감염병 예방 증명서(백신접종 증명서, 감염병 검사 증명서, 감염병 회복 증명서 등), 모바일 운전면허증, 디지털 신분증, 디지털 증명서, 사물인터넷(IoT, Internet of Things)용 증명서 등에 분산원장기술을 이용한 탈중앙화 신원관리 시스템이 적용되고 있다. 본고에서는 탈중앙화 신원증명 활용 사례를 기반으로 분산원장기술을 이용한 탈중앙화 신원관리 서비스 모델을 제안하고 그에 따르는 보안 위협을 식별한다.

2. 탈중앙화 신원관리 서비스 모델

탈중앙화 신원관리 서비스 모델은 신원증명 활용 사례에 따라 기본 모델, 수탁 및 위임 모델, 셀프발행 모델 등 3가지 유형으로 구분된다.

2.1 기본 모델



※ 출처: 서울외국어대학원대학교 자체 작성

[그림 1] 기본 모델 구성도

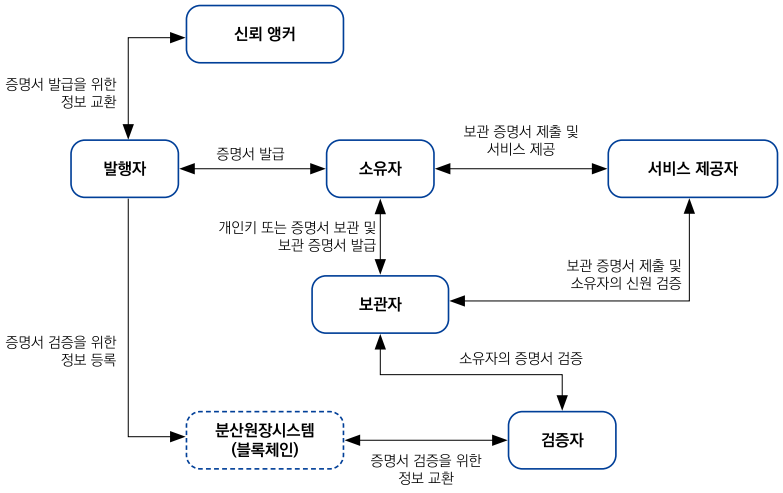
기본 모델은 신뢰 앵커(trust anchor), 발행자(issuer), 소유자(holder), 서비스 제공자(신뢰 당사자, relying party), 검증자(verifier), 분산원장시스템(블록체인) 등으로 구성된다. 본 서비스 모델을 이용한 신원증명 활용 사례는 모바일 운전면허증, 모바일 공무원증, 감염병 예방 증명서(백신접종 증명서, 감염병 검사 증명서, 감염병 회복 증명서) 등이 있다.

[그림-1]에서 보는 바와 같이, 소유자는 발행자에게 자신의 개인정보와 공개키 등을 제공하여 증명서를 발급받는다. 발행자는 증명서 발급을 위하여 신뢰 앵커(정부기관, 정부기관으로부터 권한을 위임받은 공공기관 또는 사업자 등)와 정보를 교환하고, 발급된 증명서의 검증을 위한 정보(발행자의 공개키, 소유자의 공개키 등)를 분산원장시스템(블록체인)에 등록한다. 소유자는 자신의 개인키로 서명된 증명서를 서비스 제공자(신뢰 당사자)에게 제출하고 증명서 검증이 완료되면 서비스를 제공받게 된다. 서비스 제공자가 검증자를 통하여 증명서를 검증할 때 검증자는 분산원장시스템을 통하여 증명서 검증을 위한 정보를 교환한다.

2.2 수탁 및 위임 모델

수탁 및 위임 모델은 신뢰 앵커(trust anchor), 발행자(issuer), 소유자(holder), 서비스 제공자(신뢰 당사자, relying party), 보관자(custodian), 검증자(verifier), 분산원장시스템(블록체인) 등으로 구성된다. 본 서비스 모델은 소유자가 스마트폰 등 자신의 단말기에 설치된 신원 지갑에 저장하고 있는 개인키 및 증명서의 도난이나 분실 등을 방지하기 위하여 제3자에게 위탁하고 권한을 위임하는 모델이다. 소유자는 자신의 공개키·개인키 및 증명서를 보관자에게 위탁할 수 있다. 소유자는 보관자에게 자신의 증명서 발급 권한을 위임할 수도 있다.

[그림-2]에서 보는 바와 같이, 소유자는 발행자에게 자신의 개인정보, 공개키 등을 제공하여 증명서를 발급받는다. 발행자는 증명서 발급을 위하여 신뢰 앵커(정부기관, 정부기관으로부터



※ 출처: 서울외국어대학원대학교 자체 작성

[그림 2] 수탁 및 위임 모델-1 구성도

권한을 위임받은 공공기관 또는 사업자 등)와 정보를 교환하고, 발급된 증명서의 검증을 위한 정보(발행자의 공개키, 소유자의 공개키 등)를 분산원장시스템(블록체인)에 등록한다. 소유자는 개인키 및 발급받은 증명서를 보관자에게 위탁하고 그에 상응하는 보관 증명서를 발급받는다. 소유자는 보관 증명서를 서비스 제공자(신뢰 당사자)에게 제출하고 증명서 검증이 완료되면 서비스를 제공받게 된다. 서비스 제공자는 보관 증명서를 보관자에게 제출하고 소유자의 신원을 검증한다. 보관자가 검증자를 통하여 소유자의 증명서를 검증할 때 검증자는 분산원장시스템을 통하여 증명서 검증을 위한 정보를 교환한다.

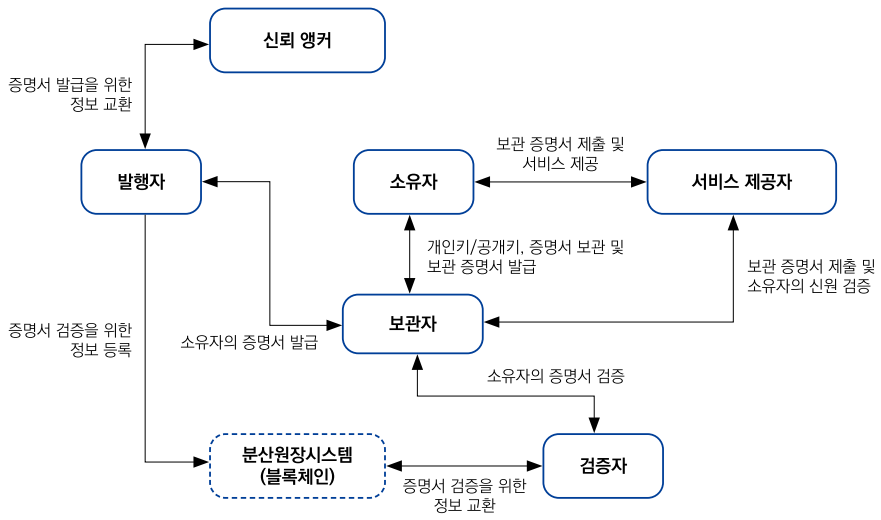
[그림-2]에서는 소유자가 발행자로부터 증명서를 발급받아 보관자에게 위탁하고 있는 반면, [그림-3]에서는 보관자가 소유자 대신에 발행자로부터 소유자의 증명서를 발급받아 보관하게 된다. 이를 위하여 소유자는 자신의 공개키도 보관자에게 위탁할 필요가 있다.

2.3 셀프발행 모델

셀프발행 모델은 소유자가 스스로 증명서를 발급하는 모델로서 발행자 및 소유자(issuer and holder), 서비스 제공자(신뢰 당사자, relying party), 검증자(verifier), 분산원장시스템(블록체인) 등으로 구성된다. 본 서비스 모델을 이용한 신원증명 활용 사례는 디지털 명함, 수업 출석 확인서, 회의·컨퍼런스·전시회 참석 증명서, 여행지 방문 확인증, 식음료 주문 확인서 등이 있다.

[그림-4]에서 보는 바와 같이, 소유자는 자신의 개인정보 등을 제공하여 직접 증명서를 발급하고, 발급된 증명서의 검증을 위한 정보(소유자의 공개키 등)를 분산원장시스템(블록체인)에 등록한다. 소유자는 자신의 개인키로 서명된 증명서를 서비스 제공자(신뢰 당사자)에게 제출하고 증명서 검증이 완료되면 서비스를 제공받게 된다.

서비스 제공자가 검증자를 통하여 증명서를 검증할 때 검증자는 분산원장시스템을 통하여 증명서 검증을 위한 정보를 교환한다. 셀프발행



※ 출처: 서울외국어대학원대학교 자체 작성

[그림 3] 수탁 및 위임 모델-2 구성도

모델에서 증명서 검증을 위한 정보를 저장·관리하기 위하여 중앙화된 데이터베이스 시스템을 이용할 수 있으나, 서로 다른 도메인에 속한 이용자 간에 신원을 증명할 때는 분산원장시스템을 이용하는 것이 상호운용성 측면에서 중앙화된 데이터베이스 시스템보다 유리하다.

2.4 보안 위협

기본 모델, 수탁 및 위임 모델, 셀프발행 모델 등 앞서 설명한 3가지 유형의 탈중앙화 신원관리 서비스에는 <표-1>에서 보는 바와 같이 잠재적 보안 위협이 존재한다. 본고에서는 통상적인 IT 서비스에서 식별할 수 있는 일반적인 보안 위협은 제외한다.

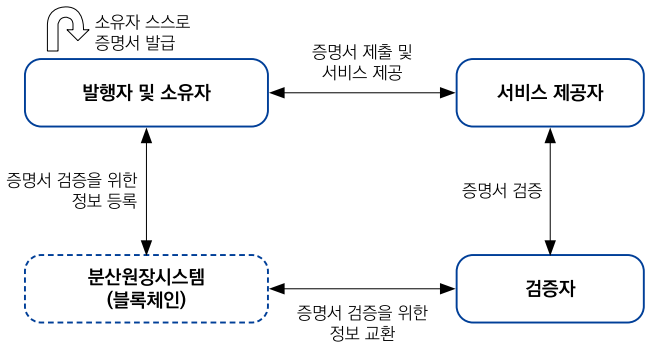
<표-1>에서 보는 바와 같이, 본고에서 제안한 탈중앙화 신원관리 서비스에 대한 주요 보안 위협은 신원 도용, 증명서 복제 및 위·변조, 증명서 제출 및 저장 시 주요 정보(개인정보, 의료정보, 금융정보 등) 유출, 수탁자(보관자) 권한 남용 등으로 구별할 수 있다.

3. 맺음말

본고에서는 최근 국내외적으로 나타나고 있는 신원증명 활용 사례를 바탕으로 탈중앙화 신원관리 서비스 모델의 유형을 3가지로 제안하였다. 기본 모델은 소유자가 발행자로부터 증명서를 발급받고 스마트폰 등 자신의 단말기에 개인키 및 증명서를 직접 저장·관리한다. 기본 모델에서 소유자는 개인키 및 증명서 도난·분실 등에 의한 신원 도용 이슈가 있기 때문에 이를 보완할 필요가 있다. 이를 위하여, 수탁 및 위임 모델에서 소유자는 자신의 개인키 및 증명서를 제3의 보관자에게 위탁하고 증명서 발급 및 검증 권한을 위임할 수 있다. 또한 소유자는 셀프발행 모델을 통하여 디지털 명함, 출석 확인서 등과 같이 보증 수준이 낮은 증명서를 직접 발급할 수 있다.

본고에서 제시한 3가지 서비스 모델에 근거하여 탈중앙화 신원관리 사업자와 이용자 등은 시스템의 복잡성, 확장성, 보안성, 구축 및 유지 비용 등의 경제성 등을 고려하여 각자의 IT 환경에 적합한 서비스 모델을 선택할 수 있다.

과학기술정보통신부 및 한국인터넷진흥원이 추진하는 분산신원증명(DID) 기술 및 표준화 포럼의 정책분과는 본고에서 제안한 서비스 모델을 대정부 정책으로 제안하였다. 또한 2021



※ 출처: 서울외국어대학원대학교 자체 작성

[그림 4] 셀프발행 모델 구성도

<표 1> 보안 위협

보안 위협	설명
신원 도용	• 발행자 신원 도용 • 제출자(소유자) 신원 도용
증명서 복제 및 위·변조	• 정적·동적 QR코드 형태의 증명서 복제 • 증명서 정보 도난·탈취 등에 의한 위·변조
증명서 제출 시 주요 정보 유출	• 주요 정보: 개인정보, 의료정보, 금융정보 등 • 정적·동적 QR코드 방식에 의한 증명서 제출 • PAN(Personal Area Network)을 이용한 단거리 무선통신(블루투스, 와이파이 다이렉트 등) 방식에 의한 증명서 제출
증명서 저장 시 주요 정보 유출	• 소유자 단말기: 개인키, 개인정보, 의료정보, 금융정보 등 저장 • 보관자 시스템: 개인키, 개인정보, 의료정보, 금융정보 등 저장
수탁자(보관자) 권한 남용	• 증명서 발급 대행: 소유자 대신 증명서 발급 • 증명서 검증 대행: 서비스 제공자(신뢰 당사자, relying party) 대신 증명서 검증

※ 출처: 서울외국어대학원대학교 자체 작성

년 9월 ITU-T SG17 국제 표준화 회의에서 한국이 제안한 신규 표준화 과제 '분산원장기술을 이용한 탈중앙화 신원관리 시스템 보안 요구사항(ITU-T X.srdidm)'이 채택되어 2024년 9월까지 한국 주도로 본고 내용을 반영한 표준안이 개발될 예정이다.

※ 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 지원에 의하여 수행됨 [과제명: 차세대 보안 표준전문연구실, 과제번호: 2021-0-00112]

참고문헌

[1] ITU-T SG17, ITU-T X.srdidm (Security requirements for decentralized identity management systems using distributed ledger technology), 2021년 9월

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

[3] ISO/TC 307, ISO/PRF TR 23249: Overview of existing DLT systems for identity management, 2021년 12월

[4] ISO/TC 307, ISO/DTR 23644: Overview of Trust Anchors for DLT-based Identity Management, 2022년 1월

[5] W3C, Decentralized Identifiers (DIDs) v1.0 (Core architecture, data model, and representations), https://www.w3.org/TR/did-core/, 2021년 8월

[6] W3C, Peer DID Method Specification (blockchain-independent decentralized identifiers), https://identity.foundation/peer-did-method-spec/, 2021년 10월

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

주요 용어 풀이

- **ITU-T SG17**: 국제전기통신연합(ITU) 산하의 전기통신표준화부문(T-섹터)에서 '정보보호' 분야 표준을 개발하는 국제 공적표준화기구
- **W3C**: 민간 기업 등 회원사가 협력하여 웹 표준을 개발하는 국제 사실표준화기구
- **NIST**: 미국 상무부 기술관리국 산하의 각종 표준과 관련된 기술을 담당하는 연구소