데이터 주권 강화를 위한 개인 간 신원확인시스템

박근덕 ITU-T SG17 Q10 부라포처,
서울외국어대학원대학교 AI블록체인연구소 교수

1. 머리말

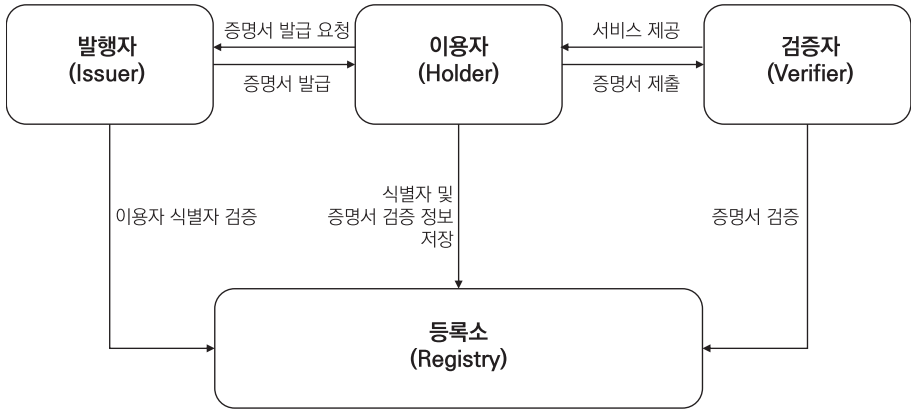
중앙화된 신원 관리에서 개인 간 신원확인은 서비스 제공자가 운영하는 개인정보처리시스템을 통하여 구현되기 때문에 개인정보 처리에 대한 보안 위협이 존재한다. 또한 탈중앙화 신원 관리에서 발행자(Issuer)와 이용자(Holder)를 분리한 서비스 모델은 신원확인 보증 수준이 높은 증명서(예: 모바일 운전면허증, 백신접종증명서 등)를 다루기에 적합하지만, 일상 생활에서 널리 사용되는 증명서(예: 명함, 수업출석증명서, 행사참석증명서, 식음료거래증명서, 여행지방문증명서 등)는 신원확인 보증 수준이 낮으므로 발행자와 이용자를 각각 분리하지 않고 이용자가 직접 자신의 개인정보 등을 입력한 증명서를 발행 및 제출하여 개인 간 상호 신원을 확인할 수 있는 서비스 모델이 필요하다. 이러한 서비스 모델은 본 표준에서 정의한 근거리 무선통신을 이용한 개인 간 신원확인시스템을 통하여 구현될 수 있다.

본고에서는 무선통신 모듈(예: Bluetooth, Wi-Fi Direct), 신원 증명서 관리 모듈, 개인정보 관리 모듈, 암호키 관리 모듈, 오프체인(Off-chain), 온체인(On-chain) 등으로 구성되는 근거리 무선통신을 이용한 개인 간 신원확인시스템을 제안한다.

2. 기존의 분산 신원 관리 서비스 모델의 문제점

기존의 분산 신원 관리 서비스 모델은 발급자(Issuer), 이용자(Holder), 검증자(Verifier), 등록소(Registry) 등으로 구성된다. 발행자는 이용자의 요청에 따라 증명서를 발급한다. 이때 증명서 유형에 따라 이용자는 발행자에게 개인정보를 제공한다. 이용자는 검증자에게 제출한 증명서를 검증할 수 있는 정보를 등록소에 저장하고, 발행자로부터 발급받은 증명서를 자신의 단말기에 저장 및 관리한다. 검증자는 등록소에 저장된 정보를 이용하여 이용자로부터 제출받은 증명서를 검증하고, 검증에 성공할 경우 이용자에게 서비스를 제공한다. 등록소는 이용자의 식별자, 이용자 증명서를 검증할 수 있는 정보 등을 저장 및 관리하기 위하여 DLT 시스템을 이용할 수 있다.

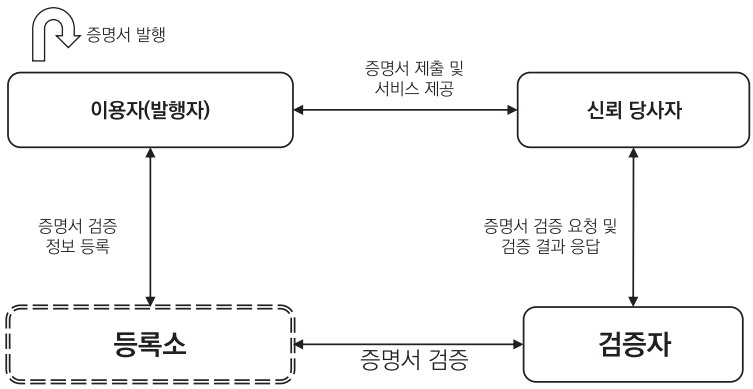
[그림 1]에 보이는 기존의 분산 신원 관리 서비스 모델은 이용자 보호 측면에서 다음과 같은 몇 가지 문제점이 존재한다.



※ 출처: 서울외국어대학원대학교 자체 작성

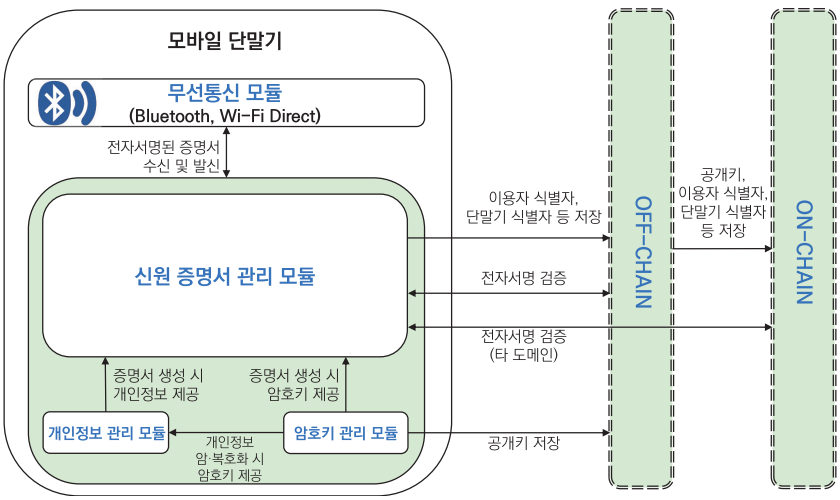
[그림 1] 기존의 분산 신원 관리 서비스 모델 구성도

- **과도한 개인정보 제공**: 이용자는 신원확인 보증 등급이 높은 증명서(예: 모바일 운전면허증, 백신접종증명서 등)를 발급받기 위하여 발행자에게 자신의 개인정보를 제공하여야 한다. 그러나 신원확인 보증 등급이 낮은 증명서(예: 디지털 명함 등)를 발급받기 위하여 발행자에게 자신의 개인정보를 제공하는 것은 과도한 개인정보 처리 행위이다.
- **과도한 개인정보 보관**: 발행자가 신원확인 보증 등급이 낮은 증명서를 발행하기 위하여 수집한 이용자의 개인정보를 보관하는 것은 과도한 개인정보 처리 행위이다.
- **손쉬운 증명서 도용**: 이용자가 큐알코드(QR code)를 활용하여 증명서를 검증자에게 제출하는 경우에 증명서 복제가 용이하고 이용자는 자신



※ 출처: 서울외국어대학원대학교 자체 작성

[그림 2] 셀프-발행 모델 구성도



※ 출처: 서울외국어대학원대학교 자체 작성

[그림 3] 근거리 무선통신을 이용한 개인 간 신원확인시스템 아키텍처

의 신원을 타인에게 제공하거나 자신의 신원을 도용당할 수 있다.

- **개인정보 유출**: 이용자가 큐알코드(QR code)를 활용하여 증명서를 검증자에게 제출하는 경우, 통상적인 큐알코드 스캐너(Scanner)를 통하여 이용자의 개인정보가 유출되기 쉽고, 유출된 개인정보를 악용한 신원 도용 등 2차 피해가 발생할 수 있다.

3. 셀프-발행 모델

셀프-발행 모델은 이용자가 직접 자신의 개인정보 등을 입력하여 신원확인 보증 등급이 낮은 증명서(예: 디지털 명함 등)를 발행할 수 있는 탈중앙화 신원 관리 모델이다. 셀프-발행 모델은 이용자(발행자), 신뢰 당사자, 검증자, 등록소 등으로 구성된다. 신뢰 당사자와 검증자는 동일한 실체가 될 수 있다.

[그림 2]에서 셀프-발행 모델의 주요 구성 요소의 역할은 다음과 같다.

이용자(발행자): 이용자 자신의 개인정보 등을 입력한 증명서를 스스로 발행하여 신뢰 당사자에게 제출하고, 제출한 증명서 검증 결과에 따라 서비스를 제공받는다. 또한 자신이 발행한 증명서를 검증할 수 있는 정보(예: 이용자의 식별자, 이용자의 공개키, 증명서 유효 기간 등)를 등록소에 등록한다.

- **신뢰 당사자**: 이용자로부터 제출받은 증명서를 검증자에게 전송하여 해당 증명서의 진위성, 유효성 등에 대한 검증을 요청한다. 검증자로부터 전송받은 증명서 검증 결과에 따라 이용자에게 서비스를 제공할 수 있다.
- **검증자**: 등록소에 등록된 증명서 검증 정보를 활용하여 이용자가 제출한 증명서의 진위성, 유효성 등을 검증하고 그 결과를 신뢰 당사자에게 전송한다.
- **등록소**: 이용자(발행자)가 등록한 증명서 검증 정보(예: 이용자의 식별자, 이용자의 공개키, 증명서 유효 기간 등)를 관리한다. 이용자가 제출한 증명서의 검증을 위하여 검증자에게 해당 증명서의 진위성, 유효성 등에 관한 검증 정보를 제공한다. 등록소는 DLT 시스템 또는 Non-DLT 시스템으로 구현될 수 있다.

4. 근거리 무선통신을 이용한 개인 간 신원확인시스템

본 근거리 무선통신을 이용한 개인 간 신원확인 시스템은 무선통신 모듈, 신원 증명서 관리 모듈, 개인정보 관리 모듈, 암호키 관리 모듈, 오프체인(Off-chain), 온체인(On-chain) 등으로 구성된다.

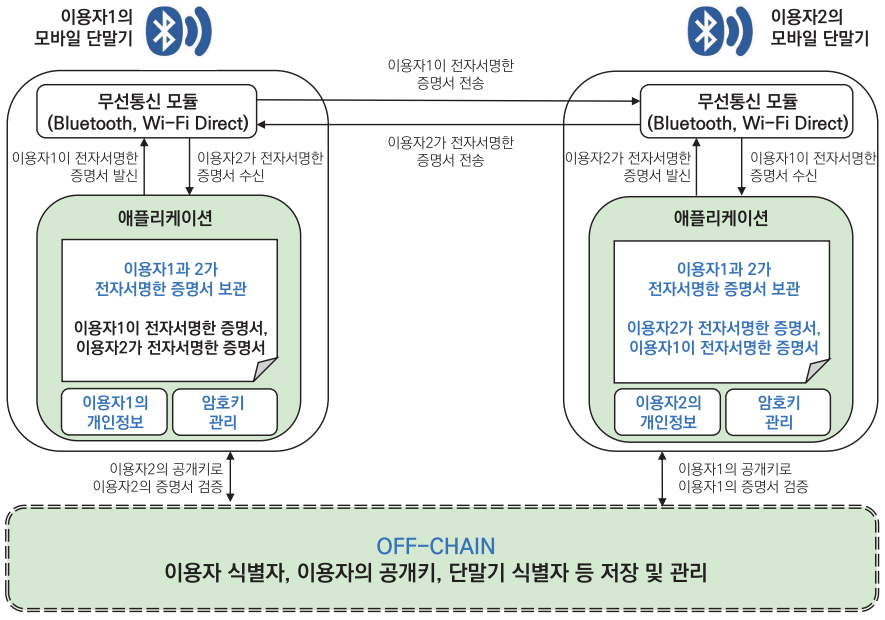
- 제안 시스템은 다음 사항을 통하여 이용자의 데이터 주권을 강화한다.
- 제안 시스템에서는 발행자(Issuer)와 이용자(Holder)가 동일한 실체이기 때문에 이용자의 증명서 발급에 필요한 개인정보를 별도의 발행자에게 제공하지 않는다.
- 이용자의 개인정보는 이용자 자신이 소유한 모바일 단말기에서만 처리되기 때문에 이용자는 개인정보에 대한 완전한 통제권을 가진다.
- 이용자의 개인정보는 오프체인, 온체인에서 처리되지 않는다.

[그림 3]에서 제안 시스템의 주요 구성 요소의 역할은 다음과 같다.

- **무선통신 모듈**: 모바일 단말기를 소유한 개인 간 신원확인을 위하여 쌍방의 신원 증명서를 근거리(예: 반경 40미터 이내)에서 무선으로 송수신한다. 모바일 단말기 간 직접 연결이 가능한 블루투스(Bluetooth)나 와이파이 다이렉트(Wi-Fi Direct)

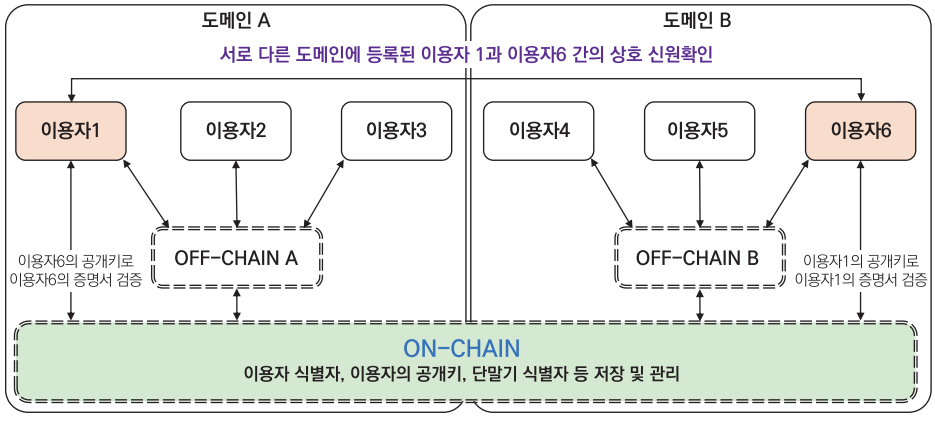
등을 이용한다. 블루투스 통신은 모바일 단말기 간 거리 측정과 저용량 데이터 전송 등에 활용될 수 있고, 와이파이 다이렉트 통신은 모바일 단말기 간 대용량 데이터 전송 등에 활용될 수 있다.

- **신원 증명서 관리 모듈**: 모바일 단말기를 소유한 개인(이용자) 간 신원확인을 위하여 자신의 신원 증명서를 생성, 저장 및 관리한다. 또한 타인의 모바일 단말기로부터 수신한 신원 증명서를 저장 및 관리한다. 신원 증명서는 이용자 자신의 개인키로 전자서명한 증명서(개인정보 포함)이다. 무선통신 모듈을 통하여 신원 증명서를 수신 및 발신한다. 이용자 식별자, 단말기 식별자 등을 오프체



※ 출처: 서울외국어대학원대학교 자체 작성

[그림 4] 동일한 도메인 내 제안 시스템 운용 구성도



※ 출처: 서울외국어대학원대학교 자체 작성

[그림 5] 도메인 간 제안 시스템의 상호 운용 구성도

인(Off-chain)에 제공한다. 오프체인 및 온체인에 저장되어 있는 정보(예: 이용자 식별자, 이용자의 공개키, 단말기 식별자 등)를 활용하여 타인의 신원 증명서의 진위성 및 유효성 등을 검증한다.

- **개인정보 관리 모듈**: 모바일 단말기의 소유자가 정보주체로서 직접 자신의 개인정보를 저장 및 관리한다. 개인정보는 암호키 관리 모듈에 보관되어 있는 암호키로 암호화 및 복호화된다. 신원 증명서 생성 시 신원 증명서 관리 모듈에 개인정보를 제공한다.
- **암호키 관리 모듈**: 모바일 단말기 소유자의 신원 증명서 생성에 필요한 전자서명을 하기 위한 공개키/개인키 쌍을 생성 및 관리한다. 또한 모바일 단말기 소유자의 개인정보를 암호화 및 복호화하기 위한 암호키를 생성 및 관리한다. 신원 증명서 생성 시 신원 증명서 관리 모듈에 개인키를 제공한다. 개인정보 암호화 및 복호화 시 개인정보 관리 모듈에 암호키를 제공한다. 공개키를 오프체인(Off-chain)에 제공한다.
- **오프체인(Off-chain)**: 동일한 도메인에 속한 개인 간 신원확인을 위하여 상대방의 신원 증명서 검증(예: 진위성, 유효성 등)이 필요한 이용자가 접근할 수 있는 저장소이다. 이용자 식별자, 모바일 단말기 식별자, 이용자의 공개키 등을 저장 및 관리하고, 이용자의 개인정보는 저장하지 않는다. 이용자의 공개키, 이용자 식별자, 단말기 식별자 등을 온체인(On-chain)에 제공한다.
- **온체인(On-chain)**: 개인 간 신원확인이 필요한 이용자가 서로 다른 도메인에 속하는 경우, 상대방의 신원 증명서 검증(예: 진위성, 유효성 등)이 필요한 이용자가 접근할 수 있는 저장소로서 이용자 식별자, 모바일 단말기 식별자, 이용자의 공개키 등을 저장 및 관리하고, 이용자 개인정보는 저장하지 않는다.

단일 도메인(예: 단일 사업자)에서 제안 시스템을 적용하는 경우, 이용자 신원 증명서를 검증할 수 있는 정보를 저장 및 관리하는 저장소로서 오프체인을 활용하더라도 이용자 간의 신원확인을 수행할 수 있고, 온체인을 활용하는 것보다 비용도 절감할 수 있다. 또한 복수 도메인(예: 복수 사업자)에서 제안 시스템을 적용하는 경우, 각 도메인별 이용자의 신원 증명서를 검증할 수 있는 정보를 저장 및 관리하는 저장소의 상호운용성을 제공하기 위하여 온체인을 활용한다.

기존 중앙화 신원 관리에서는 사업자가 이용자의 개인정보 및 신원정보를 보유하고 있어, 이용자 간 신원확인은 사업자가 수행하고 그 결과를 이용자에게 알려준다. 그러나 제안 시스템의 오프체인은 이용자의 신원 증명서를 검증할 수 있는 정보를 저장 및 관리하는 일종의 저장소 역할만 할 뿐이고, 이용자 간의 신원확인은 당사자 간에 직접 이루어지므로 탈중앙화 신원 관리의 주요한 구성 요소가 된다.

[그림 4]에서 동일한 도메인 내 이용자1과 이용자2는 서로의 신원확인을 위하여 모바일 단말기의 근거리(예: 반경 40미터 이내) 무선통신 모듈을 통하여 각각 상대방이 전자서명한 증명서를 송수신하고, 오프체인(Off-chain)에 저장되어 있는 이용자1 및 이용자2의 정보(예: 이용자 식별자, 이용자의 공개키, 단말기 식별자 등)를 활용하여 상대방의 신원 증명서를 검증한다.

[그림 5]에서 도메인 A에 등록된 이용자1과 도메인 B에 등록된 이용자6은 서로의 신원확인을 하기 위하여 온체인(On-chain)에 저장되어 있는 각자의 정보(예: 이용자 식별자, 이용자의 공개키, 단말기 식별자

등)를 활용하여 상대방의 신원 증명서를 검증한다.

4. 맺음말

본고에서 제안한 근거리 무선통신을 이용한 개인 간 신원확인시스템은 디지털 명함, 수업 출석 증명서, 행사 참석 증명서, 여행지 방문 증명서, 식음료 거래 증명서 등 서비스 구현에 활용될 수 있다. 본 제안 시스템에 대한 보안 위협 및 보안 요구사항, 활용 사례 등을 한국 주도로 2024년 9월까지 개발 예정인 ITU-T X.srdidm (Security requirements for decentralized identity management system using distributed ledger technology) 국제표준에 적극 반영할 계획이다.

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

참고문헌

[1] TTAK.KO-12.0397, 데이터 주권 강화를 위한 개인 간 신원확인시스템, 2023년 12월.

[2] ITU-T X.srdidm, Security requirements for decentralized identity management systems using distributed ledger technology, September 2023.

[3] W3C, Peer DID Method Specification, June 2023.

[4] W3C, Verifiable Credentials Data Model v1.1, March 2022.

[5] NIST, 'A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems', January 2020.

[6] 여기호, 박근덕, 염흥열, '단거리 무선 통신을 이용한 개인 간 분산 신원증명 시스템 제안', 정보보호학회논문지, 31(5), pp.923~936, 2021년 10월.

주요 용어 풀이

- ITU-T SG17: 국제전기통신연합(ITU) 산하의 전기통신표준화부문(T-섹터)에서 '정보보호' 분야의 표준을 개발하는 국제 공적표준화 기구