탈중앙화 신원증명 기반 인증 시뮬레이션 모델에 관한 연구

김호윤, 신승수*
동명대학교
miask376@gmail.com, *shinss@tu.ac.kr

A Study on the Decentralized Identifier-Based Authentication Simulation Model

Ho Yoon Kim, Seung Soo Shin*
Tongmyong Univ.

요 약

본 논문은 탈중앙화 신원증명(DID: Decentralized Identifier)에 기반하여 인증 모델에 관해 연구한다. 온라인에서 사용자 인증 기술이 고도화되고 있지만 대부분 중앙집중형식으로 해킹 공격의 주요 요인이 된다. 분산원장기술을 기반으로 하는 탈중앙화 신원증명 방법을 이용하여 중앙집중형식에서 오는 문제점을 해결하고, 공개키 암호 알고리즘을 사용하여 보안성과 무결성을 해결한다. 특히 인증 모델은 실물 신분증을 대체할 수 있기 때문에 활용도가 높다.

Ⅰ. 서 론

ICT의 발달과 함께 온라인 사용자 인증 기술 또한 고도화되면서 오프라인과 마찬가지로 온라인에서 많은 일들을 처리한다. 코로나-19로 인해 비대면으로 신원을 증명하는 일들이 많은데 이는 실물 신분증이 가지는 한계점을 드러낸다. 온라인에서 신원확인 방법은 ID와 Password를 통해서 인증하거나, 연합 신원 모델(SSO: Single Sign On, 통합로그인)을 이용하여 인증한다[1]. 이는 중앙집중화 되어 사용자에게 편리함을 제공하지만 해킹 사고 시 많은 피해가 발생한다. 중앙집중형의 문제점을 해결하기 위해 분산원장기술의 발달과 이슈로 점차 탈중앙화 시스템으로 발전하고 있다. 탈중앙화 기술이 발전하면서 DID 또한 주목받고 있는데 DID는 자기주권 신원증명을 실현할 수 있다. 탈중앙화 구조를 바탕으로 하여 사용자가 직접 자신의 ID를 관리함으로써 데이터의 주권을 ID 주인에게 부여하여 서비스 제공자가 중앙집중식으로 관리하지 않고 사용자가 직접 관리하는 권한을 가진다.

본 논문에서는 자기주권 신원증명(SSI: Self-Sovereign Identity)을 실현시킬 수 있는 탈중앙화 신원증명 인증 모델을 제안하여 사용자가 직접 ID를 관리하고 데이터의 주권을 ID 주인에게 직접 부여한다[2,3].

Ⅱ. 관련연구

2.1 분산원장기술

분산원장기술은 P2P(Peer-to-Peer) 기술을 기반으로 신뢰할 수 있는 제3자 없이도 데이터를 분산 저장 및 공유하고, 동일한 데이터를 유지하여 무결성을 보장하는 기술이다. 분산원장은 블록체인을 구성하는 가장 중요한 요소 중 하나이며, 블록체인을 탈중앙화된 시스템으로 만들어주는 핵심 기술이다. 거래 기록 등의 데이터를 저장하는 데이터베이스를 중앙화된 서버가 소유하는 것이 아니라, 블록체인에 참여하는 모든 사람이 동일한 원장을 소유하고 관리하는 기술을 일컫는다. 분산원장의 특징은 모든 정보가 암호화되어 Append-only 방식으로만 원장에 저장되기 때문에 한 번 원장에 기록된 정보는 절대 수정할 수 없다. 불가변성의 특성은 블록체인 데이터에 대한 악의적인 변조를 불가능하게 만들어서 데이터에 대한 신뢰도를 향상시켜 준다[4].

2.2 DID

DID는 분산원장기술에 기반한 신원증명이며, 중앙 시스템으로부터 통제받지 않고 개인이 자신의 정보에 대해 통제권을 갖게 하는 디지털 신원관리 체계이다. DID는 DID 주소값과 1:1 관계를 가지는 DID document가 있고, DID document는 분산저장소에 저장한다. 분산저장소는 주로 블록체인을 사용하며 Bitcoin, Ethereum과 같은 비허가형 네트워크뿐만 아니라 Hyperledger와 같이 허가형 네트워크도 사용한다. DID document는 DID 소유 인증에 사용되는 PublicKey 값을 포함한다. DID는 DIF(Decentralized Identity Foundation)의 주도로 개념과 설계가 세워졌고, W3C(World Wide Web Consortium)가 주도하에 국제 표준(Decentralized Identifiers Standards)이 제정되고 있다[5].

Ⅲ. 인증 시뮬레이션 모델

3.1 모델 구성

모델의 주요 참여자는 발행기관(Issuer), 사용자(Holder), 검증인(Verifier), 그리고 DID 관련 정보를 저장하는 분산저장소로 Verifiable Data Registry가 있다. 발행기관은 신뢰기관으로써 사용자가 요청한 신원증명을 DID를 통하여 검증 후 발행한다. 사용자는 신원증명을 필요한 항목만으로 검증인에게 제출하기 위해 재가공한다. 검증인은 서비스 제공자이며 사용자로부터 제공 받은 신원증명의 진위 여부를 분산저장소를 통해 검증한 뒤 서비스를 제공한다.

3.2 구성 요소

사용자와 사용자 인증을 위해 이용되는 DID와 DID document가 있

고 사용자가 발행기관으로부터 발급받는 신원증명 ID 속성으로 VC(Verifiable Credential), 그리고 검증인에게 제출하기 위해 제공 ID 속성으로 VP(Verifiable Presentation)가 있다. VC 항목은 발행기관의 정보, 속성 값, 그리고 발행기관의 서명 데이터가 포함되며 그림 Fig. 1과 같다.

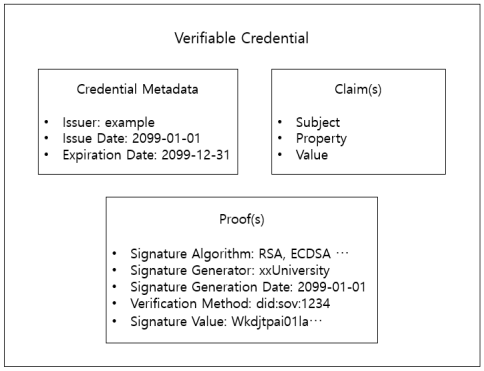

Fig. 1. VC Element

3.3 모델 시나리오

먼저 발행기관과 사용자는 DID Auth를 하기 위한 DID 생성과 공개키를 각각 생성한다. 사용자는 발행기관에 VC(Verifiable Credential) 발급을 요청하고 발행기관은 모바일 본인인증, I-PIN 등 1차 인증을 수행한다. 그리고 사용자의 DID를 통해 DID document 위치를 확인하여 획득한다. DID document를 획득한 뒤 Challenge를 생성하고 사용자에게 DID Auth를 요청한다. DID Auth통해 인증 후 사용자에게 VC를 발급해준다. 사용자는 발급받은 VC를 검증자에게 필요한 항목만으로 제출하기 위해 VP(Verifiable Presentation)로 가공하여 제출한다. 검증자는 제출 받은 VP를 검증하기 위해 Proof 항목으로 분산저장소를 통해 검증한다. 모델의 흐름도는 Fig. 2와 같다.

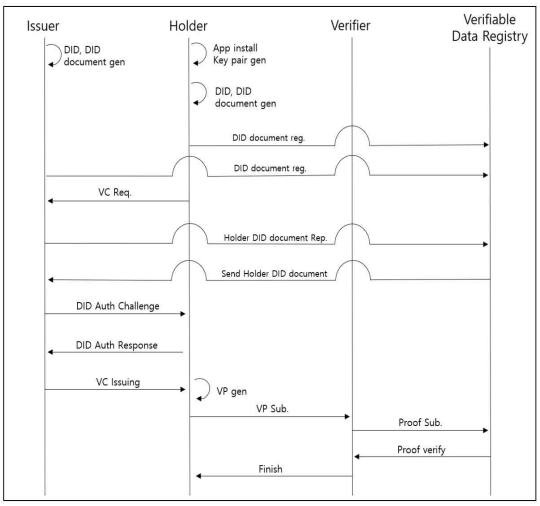

Fig. 2. Proposed System Flow Chart

DID Auth는 매번 다른 값의 Challenge로 진행되며 발행기관은 임의의 난수 값을 생성하여 사용자에게 보낸 뒤 약속된 암호 알고리즘으로 암호화하여 Response를 전달하고 결과 값을 비교해 인증을 수행한다. 이는 스니핑과 재사용 공격에 안전하고, PKI기반으로 중간자 공격에도 안전하다.

Ⅳ.결론

온라인에서 나를 증명하는 신분 확인 기술은 매우 중요하다. 본인인증은 다양한 기술을 이용하여 구현하지만 여전히 문제점이 있다. 기술이 발전함에 따라 편리하면서 보안 위협을 낮출 필요성이 있다. 본 논문에서는 탈중앙화 신원증명 기반 인증 모델을 제시하여 사용자의 데이터 주권을 강화하고자 한다. 제안 모델은 실물 신분증을 대체할 수 있으며 단순히 신분증을 모바일로 옮기는 것이 아닌 분산원장에 DID를 등록 후 필요 시 전자 신분증을 꺼내 이용하여 자기주권 신원증명을 실현하고자 한다. 향후 연구로는 플랫폼 간에 호환성 문제 해결과 표준화 작업에 대한 연구가 필요하다.

ACKNOWLEDGMENT

“This research was supported by the BB21plus funded by Busan Metropolitan City and Busan Institute for Talent & Lifelong Education(BIT).”

참 고 문 헌

[1] W. Li & C. J. Mitchell. (2020). User Access Privacy in OAuth 2.0 and OpenID Connect. IEEE EuroS&PW.

[2] Sovrin Protocol and Token White Paper. (2018). Sovrin Available online: https://sovrin.org/제-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

[3] What is self-sovereign identity. (2018). Sovrin Available online: https://sovrin.org/faq/what-is-self-sovereign-identity

[4] J. K. Lee. (2020). Hyperledger Fabric Configuration and Channel Development Case Study for Google Cloud-based Distributed Ledger Processing. Korean Association Of Computers And Accounting, 18(1), 19-39.

[5] Decentralized identity Foundation. (2019). DIF. https://identity.foundation