DID에서 사용자 비연결성을 제공하기 위한 일회용 DID에 관한 연구

김태훈[1], 김수현[2], 이임영[2]
[1]순천향대학교 소프트웨어융합학과 박사과정
[2]순천향대학교 컴퓨터소프트웨어공학과 교수
20134101@sch.ac.kr, kimsh@sch.ac.kr, imylee@sch.ac.kr

A Study on One-Time DID for Providing User Unlinkability in DID

Taehoon Kim[1], Su-Hyun Kim[2], Im-Yeong Lee[2]
[1]Dept. of Software Convergence, Soonchunhyang University
[2]Dept. of Computer Software Engineering, Soonchunhyang University

요 약

디지털 신원은 온라인 환경에서 빠르게 중요해지고 있으며, 그 관리의 중요성은 날로 커지고 있다. 중앙화된 신원 관리 시스템의 한계를 인식하며, 탈중앙화된 신원 관리 시스템인 DID(Decentralized Identifier)에 대한 연구와 관심이 확대되고 있다. 그럼에도 불구하고, DID 활용 시 개인정보 유출의 리스크는 여전히 남아 있다. 이러한 문제를 해결하기 위해, 본 연구는 일회용 DID 기법을 제시하였고, 해당 기법은 사용자의 비연결성을 향상시키며, 키 유출과 관리 문제를 최소화한다. 본 연구를 통해, 일회용 DID가 비연결성 강화, 키의 안전한 관리 등의 이점을 제공함을 확인하였다.

1. 서론

디지털 신원은 온라인 환경에서 개인이나 기기의 고유성을 표현하는 중요한 요소이다. 그러므로 디지털 신원에 대한 관리는 매우 중요하며, 오랜 시간 동안 중앙화된 시스템과 프로토콜을 기반으로 관리되었다. 그러나, 이러한 중앙화된 시스템은 보안 취약성, 데이터 소유권 문제, 중앙화된 시스템의 신뢰 문제 등 다양한 문제점들을 가지고 있다.

이러한 문제점들을 해결하기 위해 탈중앙화된 신원 관리 시스템의 필요성이 대두되었다. 그 중에서도 DID(Decentralized Identifier)는 중앙 기관 없이 개인이 스스로 고유 신원을 선택적 공개 및 제시하고 관리할 수 있다. 이는 개인정보 보호와 데이터 주권의 강화로 인해 많은 주목을 받고 있다[1].

그러나, DID를 사용함에 있어 개인정보 유출의 위험은 여전히 존재한다. 특히, 다양한 서비스에 접근하기 위해 여러 VP(Verifiable Presentation)를 제시할 때, 서비스 제공자는 동일한 DID를 기반으로 사용자의 다양한 VP 정보를 연결하거나 추적할 수 있게 된다[2].

본 연구에서는 이러한 문제를 해결하기 위해 일회용 DID 기법을 도입하여 사용자의 비연결성을 강화하였다. 이 방법을 통해, 서비스 제공자는 여러 VP 정보를 수집하더라도 그 정보들이 동일한 사용자에게 속하는지를 연결하거나 추적하는 것이 불가능해진다.

2. 제안방식

2.1 설정 단계

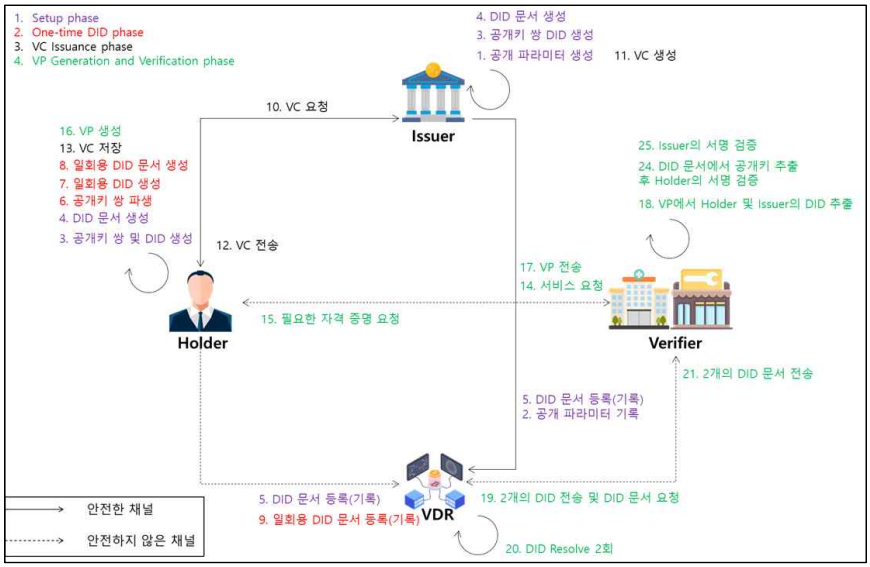
Issuer가 공개 파라미터들을 생성하고, 생성한 공개 파라미터들을 VDR(Verifiable Data Registry)에 기록한다. 이후 DID의 각 참여자들(Issuer, Holder 등)은 자신의 ECC(Elliptic Curve Cryptography) 기반의 공개키 쌍을 생성하고, 공개키를 입력으로 DID를 생성한다. 그리고 DID의 참여자들은 자신의 공개키와 DID로 구성된 DID 문서를 생성한 후 이를 VDR에 게시한다.

2.2 일회용 DID 생성 단계

Holder는 일회용 DID를 사용하고 싶을 경우 기존의 공개키 쌍, 체인코드, 인덱스, 지식 기반 패스워드를 이용하여 공개키 쌍을 파생한다. 그리고 파생된 공개키를 입력으로 일회용 DID를 생성한다. 그리고 생성한 파생된 공개키와 일회용 DID로 구성된 DID 문서를 생성한 후 이를 VDR에 게시한다.

2.3 VC 발급 단계

Holder는 Issuer에게 자신의 자격 증명을 전송하



(그림 1) 본 연구의 전체 시나리오

면서 VC(Verifiable Credential) 발급을 요청한다. 그리고 Issuer는 수신한 자격 증명의 진위를 확인하고, 올바른 경우 VC를 생성하여 Holder에게 발급한다. 진위가 올바르지 않다면 reject한다.

2.4 VP 생성 및 검증 단계

Holder가 Verifier로부터 서비스를 요청하고, Verifier는 이에 필요한 자격 증명을 요구한다. 그리고 Holder는 요청한 자격 증명이 포함된 VC들을 구성하여 VP를 생성하고, 이를 Verifier에게 제시한다. 이후 Verifier는 VP를 검증하며, 검증이 올바르다면 Holder에게 서비스를 제공한다.

3. 제안방식 분석

- **사용자 비연결성**: 본 연구는 VP마다 각기 다른 Holder의 일회용 DID로 구성되어 있으므로 서비스 제공자는 여러 VP들을 수집 및 분석하여도 Holder를 연결하거나 추적하는 것이 불가능하다.
- **키의 유출 방지**: 본 연구는 기존의 BIP-32에서 지식 기반 패스워드를 입력 파라미터로 추가하여 연산을 수행하기 때문에 체인코드 및 인덱스가 유출되어도 키의 유출이 불가능하다.
- **키 관리 문제 방지**: 기존의 비결정적 키 생성 방식은 많은 수의 키 쌍을 관리해야 하지만 본 연구는 개선된 BIP-32를 사용하기 때문에 보다 적은 수의 공개키 쌍으로 생성, 관리 할 수 있다.

4. 결론

데이터 주권과 개인정보 보호가 중요한 가치로 여겨짐에 따라 탈중앙화된 신원 관리 시스템인 DID가 대두되었다. 그러나, DID를 활용하는 과정에서도 여전히 개인정보의 유출 위험성이 존재하는 것이 문제로 제시되었다. 본 연구는 이 문제에 대한 해결책으로 일회용 DID 기법을 제안하였으며, 사용자의 비연결성 강화, 키의 유출 방지, 효율적인 키 관리라는 세 가지 주요 특징을 중심으로 제안방식 분석을 통해 확인하였다.

향후 연구 방향으로는 본 연구의 방법론을 실제 서비스에 구현하는 개발 단계를 포함해야 하며, 제안된 키 생성 방식 외에 BIP-39, 44 등의 사용 가능성에 대해서도 논의되어야 한다.

Acknowledgment

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(RS-2022-00167197, 스마트시티 구축을 위한 지능형 5G/6G 핵심 인프라 기술 개발)과 한국연구재단 4단계 두뇌 한국21사업(4단계 BK21사업) (과제번호:5199990914048), 문화체육관광부 및 한국콘텐츠진흥원의 2023년도 SW저작권 생태계 조성 기술 개발 사업으로 수행되었음 (과제명 : 클라우드 서비스 활용 구축 형태별 대규모 소프트웨어 라이선스 검증 기술개발, 과제번호 : RS-2023-00224818, 기여율: 50%)

참고문헌

[1] Reed, D. et al., “Decentralized identifiers (dids) v1. 0.”, Draft Community Group Report, 2020.

[2] Sporny, M. et al., “Verifiable Credentials Data Model v2.0”, Draft Community Group Report, 2023.