자기주권 신원 기반 피어-투-피어 통신 메커니즘 분석

최규현*, 김근형*
*동의대학교 게임공학전공
giry8647@gmail.com, geunkim@deu.ac.kr

An analysis on Peer-to-Peer communication mechanism based on self-sovereign identity

Gyu-Hyun Choi*, Geun-Hyung Kim*
*Game Engineering Major, Dong-eui University

요 약

자기 주권 신원 증명 기술인 DID가 강력한 인증 수단으로 떠오르고 있다. 이런 DID 기술을 사용한 DIDComm은 중앙을 거치지 않는, 사용자끼리의 통신(P2P)을 가능하게 만들어 주며, 이는 강력한 보안을 제공해 준다. 본 글은 DIDComm 기술을 활용한 P2P 메신저에 대해 작성하였다. 이를 활용한 메신저는 사용자 간의 높은 보안을 가진 통신을 제공해 줄 수 있으며 앞으로의 인터넷 시대, 메타버스 시대에서 주목할 만한 기술이다.

1. 서론

최근 블록체인기술을 활용한 여러 기술이 나오고 있으며, 그중 탈중앙화를 기반으로 하는 인증 시스템인 DID(Decentralized Identifier) 기술이 떠오르고 있다. DID 기술이 떠오르는 이유는 기존에 사용되던 시스템들의 한계와 해킹 문제 때문이다. 기존의 시스템의 경우 특정한 중앙에 자신의 정보를 제공하는 것으로 자신을 증명하였는데, 이는 특정한 중앙에 개인 정보가 몰리는 현상을 발생시켰고, 자신의 정보를 맡긴 중앙이 해킹을 당하는 것으로 본인의 의사와 상관없이 개인 정보가 유출되거나, 중앙이 사용자 정보를 임의로 사용하는 등의 여러 가지 문제점들이 나오기 시작했다. 그리고 인터넷 사용자가 증가하면서 인터넷에서 사용되는 개인 정보량도 증가하였고, 그에 따라 해킹으로 인한 피해 규모 또한 늘어나고 있다[1].

DID 기술은 이러한 문제들을 해결하기 위해 개인의 정보를 특정한 기관이 통제하는 것이 아닌, 본인이 통제하는 것으로 본인의 개인 정보를 스스로 관리하며 인증을 가능하게 만드는 자기 주권 신원(Self Sovereign Identity)을 가능하게 만들어 주었다[2].

이러한 DID를 사용한 통신 방법인 DIDComm 또한 같은 이유로 만들어졌다. 사용자 간의 통신에서 중앙을 거치지 않는 것으로 중앙의 관여를 배제할 수 있다. 이러한 기술은 앞으로 더 발전할 인터넷 환경에 강력한 인증 및 통신 시스템을 제공해 줄 것이고, 더 나아가서 새로운 메타버스 시대에 강력한 자기 인증 수단과 통신 수단을 제공해 줄 것이다.

본 글은 위와 같은 DID를 통신에 접목한 DIDComm을 활용한 peer-to-peer(이하 P2P) 메신저를 분석한 내용을 작성하였다.

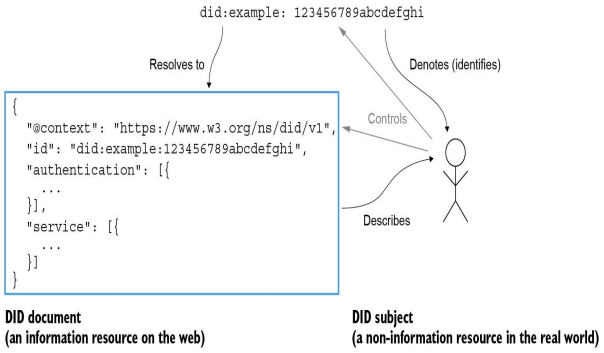
2. 자기주권 신원 기반 P2P 통신 메커니즘

2.1 분산 식별자(DID: decentralized identifier)

분산 식별자(DID: decentralized identifier)는 자기주권 신원 시스템에서 검증가능 자격증명의 핵심요소로 W3C에서 표준이 이루어진 새로운 유형의 식별자이다. 분산 식별자는 중앙 기관에 무관하게 소유자가 생성한 특별한 종류의 식별자이다. 분산 식별자는 다음의 식별자에 관한 요구사항을 모두 만족한다.

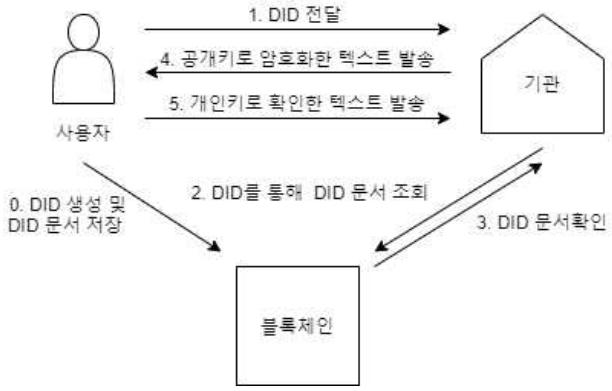
- 탈중앙화: 식별자의 중앙 발행기관이 없어야 한다.
- 영속성: 본질적으로 영구적이어야 하며 하부 기관의 지속적인 운영을 요구하지 않아야 한다.
- 암호로 검증 가능: 식별자의 제어권을 암호로 증명할 수 있어야 한다.
- 해석 가능: 식별자에 대한 메타데이터를 검색할 수 있어야 한다.

분산 식별자로 식별되는 개체를 인증하기 위해서 분산 식별자 하나에 관련된 공개키(public key)와 개인키(private key) 쌍이 이용된다. 분산 식별자는 블록체인 또는 다른 탈중앙 네트워크에 저장된 공개키의 주소 역할을 한다. 모든 분산 식별자는 관련된 하나의 DID 문서가 있다. DID 문서에는 DID 주체에 대한 메타데이터가 포함된다. 이 메타데이터는 분산 식별자에 의해 식별되는 DID 문서에 의해 설명되는 자원에 대한 용어이다. 예로 개인에 대한 분산 식별자에는 일반적으로 암호화 키, 인증방법 및 통신할 대상자와 신뢰할 수 있는 상호작용에 참여하는 방법을 설명하는 메터데이터를 포함하는 DID 문서를 가진다. 분산 식별자와 DID 문서를 제어하는 엔티티를 DID 컨트롤러라 한다. (그림 1)은 DID 컨트롤러가 DID 주체와 동일한 경우의 분산 식별자와 DID 문서와의 관계를 보인다.



(그림 1) DID, DID 문서, DID 주체와의 관계

자기주권 신원 시스템에서 분산 식별자의 인증은 다음과 같이 진행된다[2]. 먼저 사용자는 인증이 필요한 기관에 분산 식별자를 전달하고 기관은 전달받은 분산식별자를 통해 블록체인에 저장된 DID 문서를 얻은 후 DID 문서 내의 사용자의 공개키를 활용하여 특정 메시지를 암호화하여 사용자에게 전달한다. 전달받은 사용자는 기관에서 전송한 특정 메시지를 비밀키로 복구하여 확인하고 사용자가 확인한 메시지를 개인키를 암호화하여 기관에 전달하는 것으로 분산 식별자의 인증이 완료된다.



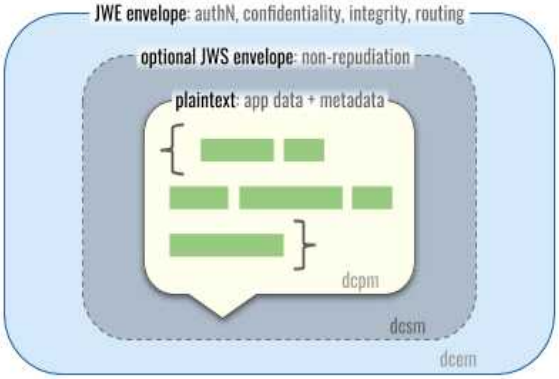
(그림 2) 사용자의 분산 식별자 인증(DID Auth) 절차

분산 식별자 인증은 상대방에게 분산 식별자에 대한 소유권을 증명하는 과정으로 분산 식별자 소유자가 개인키를 제어할 수 있음을 증명함으로써 자신을 인증하는 표준이다. 분산 식별자 인증을 위해서 DID 문서에 포함된 공개키와 인증(authentication) 항목 등을 사용한다.

2.2 DIDComm

DIDComm은 분산 식별자의 분산 설계를 기반으로 구축된 안전하고 암호화된 통신 방법을 제공하는 것이 목적이다. DIDComm은 사람, 기관 또는 사물에 의해 제어되는 소프트웨어 간의 보안 통신 채널(secure communication channel)을 생성한다. DIDComm은 인증된 채널을 구성하며 주어진 분산 식별자의 개인키에 대한 제어가 해당 분산 식별자가 대표하는 당사자의 진위를 증명하는 것이다. DIDComm구조는 통신에 참여하는 모든 주체가 신뢰적인 통신을 위해 상호인증(mutual authentication)하는 방법을 제공한다. DIDComm의 기본 패러다임은 메시지 기반, 비동기식, 단 방향 통신으로 세션 개념을 가지지 않는다.

DIDComm은 DID를 사용한 메시지인 DIDComm 메시지 타입을 정의하고 있으며 DIDComm이 제공하는 API를 사용하는 것으로 메시지를 만들고 암호화, 복호화, 메시지를 읽는 것을 가능하게 한다.

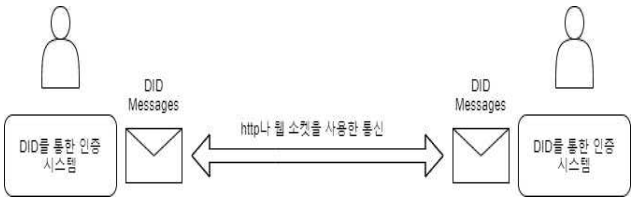


(그림 3) DIDComm 메시지 구조.

DIDComm을 사용한 통신을 할 경우 다음과 같이 진행된다[3]. 통신을 원하는 두 사용자는 상대방의 DID를 수신하고 수신한 DID를 기반으로 DID 문서를 확인, DID 문서에 작성되어있는 공개키와 서비스 종단점을 통해 서로 연결이 가능해지며, 특정한 텍스트를 서로의 DID 문서의 공개키로 암호화하여 전송, 이를 개인키로 풀어 확인하여 인증하는 것으로 서로에 대한 인증까지 가능하게 만들어 준다. 하지만 위와 같은 통신의 경우 DID의 유효성만의 인증을 해주기 때문에 DID 사용자의 인증까지 필요한 경우 해당 사용자를 인증해 줄 인증기관과의 연결이 추가되어야 하며, 이 과정에서 인증기관을 확인하는 절차를 추가할 수도 있다.

2.3 DIDComm을 사용한 P2P 통신

DIDComm의 특징을 사용할 경우 중앙을 거치지 않고 사용자끼리의 통신(P2P)을 가능하게 만들어 준다. 그리고 이런 DIDComm을 P2P 통신에 사용하면 높은 보안 수준의 통신 환경을 제공해 준다. DIDComm을 P2P 메신저에 사용한다면 다음과 그림과 같은 모양이 된다.



(그림 4) DIDComm 메시지를 활용한 P2P 통신 예.

2.4 기존 방식과의 차이점

DIDComm을 이용한 P2P 통신은 중앙인 서버가 필요하지 않다. 이는 서버의 유무가 통신에 큰 영향을 끼치지 않으며, 서로가 메신저를 가지고 있고 통신 가능한 환경에 있다면 어디서든 통신을 할 수 있다. 기존의 방식은 서버를 통해 서로 연결을 주고받았으며, 이 과정에서 중앙인 서버의 개입이 필요했다. 서버의 유무가 연결에 영향을 끼쳤으며, 통신에 사용된 정보에 관여하는 것 또한 가능했다. 이는 앞에서 말한 바와 같이 중앙의 해킹으로 인한 개인 정보 유출이나 개인 정보 무단 사용 등의 문제를 일으킬 수 있다. DIDComm을 사용한 메신저는 중앙의 개입을 없애는 것으로 위와 같은 문제들을 해결하였다.

그러나 이러한 통신 방법은 개인에 의해 연결되기 때문에 그만큼 개인의 책임이 커진다. 중앙을 거친 통신의 경우 중앙에서 사람들을 관리해주는 것으로 사기 등의 문제를 어느 정도 제어하는 것이 가능하며, 대화 기록 등을 저장해 두는 것으로 대화 내용을 복구하는 등의 일들이 쉬워진다. 하지만 중앙의 개입이 없는 사용자간의 통신의 경우 통신 연결에서 문제가 생길 경우 문제를 파악하고 해결하는 것에 어려움이 있을 것이며, 사기 등의 피해를 미연에 방지하는 것이 어렵다.

이러한 문제를 보안하기 위해선 개인 간의 통신에서 신뢰를 위해 추가적인 정보 교환을 추가하거나, 중간에 중개자를 두는 것으로 보완할 수 있다.

3. 결론

본 글은 DIDComm 기술을 활용한 P2P 메신저에 대해 작성하였다. DID 기술을 활용한 DIDComm은 앞으로 발전할 인터넷 세계에 강력한 보안을 가진 통신을 제공해 줄 것이다. 그리고 이를 활용한 메신저는 떠오르고 있는 메타버스 시대에서 주목할 만한 통신 방법이다. 중앙을 통하지 않기 때문에 서로 메신저만 있다면 통신이 가능해지며, 이를 사용하여 개인적인 대화나 거래에도 사용할 수 있다. 하지만 DID를 사용한 통신은 그만큼 중앙의 개입이 적어지므로 개인의 책임이 커지며, 만약에 거래를 통해 피해를 볼 경우, 그에 대한 본인의 책임 또한 매우 커질 것이다. 이를 보안하기 위해 개인 간의 신용을 위한 정보 교환을 추가하는 방법을 고려해볼 수 있다.

감사의글

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원 및 교육부와 한국연구재단의 재원으로 지원을 받아 수행된 사회맞춤형 산학협력 선도대학(LINC+) 육성사업의 연구결과임. (No. NRF-2021R1F1A1047573).

참고문헌

[1] 김영현. "블록체인을 활용한 디지털 신원증명 적용방안 연구." 국내석사학위논문 국민대학교 소프트웨어융합대학원, 2020. 서울

[2] 윤대근 "자기주권 신원증명 구조 분석서" 제이펍 2020

[3] Sam Curren (Indicio), Tobias Looker (Mattr), Oliver Terbu (ConsenSys) "DIDComm Messaging" https://identity.foundation/didcomm-messaging/spec/