탈중앙형 신원 식별 서비스 기반 안전한 접근 제어 기법에 관한 고찰

조강우*, 정병규*, 신상욱**

*부경대학교 대학원 정보보호학과 (대학원생)

**부경대학교 IT융합응용공학과 (교수)

A Study on Secure Access Control Management Based on Decentralized Identification Service

Kang Woo Cho*, Byeng-Gyu Jeong*, Sang Uk Shin**

*Dept. of Information Security, Graduated School,

Pukyong National University (Graduate Student)

**Dept. of IT Convergence and Application Eng.,

Pukyong National University (Professor)

요 약

급증하는 차세대 신원 식별 서비스 수요에 따라 안전한 탈중앙형 ACM 기법에 대한 요구가 상응하였다. 이에 따라 탈중앙형 신원 식별 서비스에 기반하는 다양한 ACM 기법이 제안되었으나 대부분 연구 도입기에 해당한다. 본 논문에서는 탈중앙형 신원 식별 서비스에 대한 개요에 대하여 논하고 안전한 ACM 기법의 요구사항 및 현행 연구 동향에 관한 고찰을 수행하며, 결과적으로 탈중앙형 신원 식별 서비스 기반 안전한 접근 제어 기법에 대한 연구 시사점을 제공한다.

I. 서론

다양한 신원 식별 기법이 탈중앙 서비스 형태로 변화함에 따라, 기존 중앙 집중 형태의 신원 식별에서 활용하던 접근 제어 관리(Access Control Management, ACM) 기법의 변화가 요구되었다. 중앙 집중형 ACM의 경우 일괄적으로 저장되는 신원 데이터에 대한 효율적인 정책 관리가 가능하며, 모든 네트워크 참여자가 신뢰하는 정책에 따른 접근 권한 분배가 용이했다. 하지만 탈중앙 형태의 신원 식별은 신원 데이터를 분산된 원장에 기록하며, 상호 비신뢰 관계의 P2P(Peer-to-Peer) 네트워크를 형성하기 때문에 이러한 기존 ACM 기법을 적용하는 것에 다수의 제약이 잇따른다.

탈중앙형 신원 식별 기법 연구는 단순한 DID(Decnetnralized IDentity) 형태에서 발전하여 DIDs(Decentralized IDentifiers)를 포함한 SSI(Self-Sovereign Identity) 기술로 변화한다. 현행 연구의 초점은 탈중앙 기술에 범용적으로 적용 가능한 ACM 기법을 개발하는 것에 있다.

본 논문에서는 2장에서 탈중앙형 신원 식별에 대한 배경지식을 제시한다. 3장에서는 탈중앙형 신원 식별에 대한 안전한 ACM 기법의 요구사항을 도출하고 이를 바탕으로 기존 제안된 탈중앙형 신원 식별 기반 ACM 관련 연구를 논하며, 4장에서 결론을 제시한다.

II. 탈중앙형 신원 식별

탈중앙형 신원 식별은 식별자와 신원으로 분류된다. 그 중 식별자 기술에 해당하는 DIDs는

실질적인 탈중앙형 동작을 가능하게 하는 기술이다[1]. 이는 지시된 신원 데이터에 식별자 태깅을 통해 정확한 신원 식별을 제공하며, 나아가 안전한 로컬 스토리지에 저장되는 신원 데이터에 탈중앙 속성을 부여한다. 일반적인 DIDs Resolver는 다음의 형식을 따른다.

did : [method] : [identifier]

한편, DIDs를 사용하는 SSI는 검증 가능한 자격 증명인 VC(Verfiable Credential)을 포함한 탈중앙형 신원 식별 솔루션이다. 신원 검증을 위한 방법으로 VC를 VP(Verifiable Presentation)로 2차 가공하는 것을 통해 정보 주체의 강력한 선택권, 삭제권 등의 자기 주권형 동작을 보장하는 것이 특징이며, 영지식 증명(Zero-Knowledge Proof) 등을 통해 신원 데이터를 안전하게 거래할 수 있도록 고안되었다. 또한, 데이터 거래 환경에 Steward-Ownership 기반 프라이빗 블록체인 네트워크를 도입하는 것으로 탈중앙형 동작을 달성하며 네트워크에 참여하는 각 노드가 상호 비신뢰 관계에서도 DID 검증을 통해 증명인-발행인-검증인으로 구분되는 역할을 유동적으로 수행할 수 있다.

현행 SSI 연구로는 Linux 재단의 Hyperledger Indy 프로젝트 일종인 SOVRIN, Etherium 기반 uPort, Jolocom 등을 비롯하여 ShoCard, OmniOne 등 다수 존재하며, 이들은 상이한 자체 개발 ACM 기법을 채택하였다[2].

III. DIDs/SSI 기반 안전한 접근 제어

3.1 요구사항

일반적인 ACM의 요구사항은 다음과 같다[3].

1. 최소 권한 : 사용자가 수행할 작업에 필요한 권한만이 역할에 부여된다.
2. 직무 분리 : 집근 제어 관리자가 접근 권한을 스스로 부여하는 것을 방지하기 위해 상호 배타적 역할을 호출할 수 있어야 한다.
3. 컨텍스트 기반 권한 : 접근 제어 결정을 계산하는데 반드시 필요한 정보만을 저장하고 처리한다.

하지만 SSI는 ID의 관리 권한을 개인에게 부여하기 때문에 개인 중심형 ID 기술로 분류된다. 따라서 이는 중앙 집중식 기관이 존재하지 않기 때문에 기존의 ID 관리와는 대조적인 개념으로, 다음과 같은 탈중앙 형태의 요구사항을 추가적으로 지닌다[4].

1. 참여자 선택 : 접근 제어 정책에 합당한 VC를 보유한 사용자만이 권한 부여의 자격을 지닌다.
2. 데이터 기밀성 : 접근 제어 엔진은 ZKP를 통해 최소한의 정보만을 기반으로 의사 결정을 수행한다.
3. 책임 및 부인 방지 : 발행인은 발행한 VC에 대한, 검증인은 검증한 VC에 대한 책임을 지닌다. 동시에 상호 비신뢰 관계의 탈중앙 네트워크에서 신원 식별과 검증에 대한 송수신 측 및 서비스 종단점에서의 부인이 불가능하여야 한다.

3.2. SSIBAC

SSIBAC은 인증 및 자격 증명 발급을 위한 SSI 모델에서 사용자 데이터 프라이버시 및 주권에 초점을 맞춘 ACM 기법 제안이다[4]. 이는 사용자가 데이터에 접근하기 위해 컨텍스트 기반 권한 VC를 PRP(Policy Retrieval Point)에 저장하는 것으로 기존 중앙 집중형 ACM에서 사용하던 접근 제어 정책을 블록체인 기반 SSI 솔루션에 이식하는 것을 목표로 한다.

이는 발행인에 의해 발행된 VC를 증명인이 VP로 생성하기 위해 분산 원장으로부터 Schema 요소를 획득하는 시점에서 접근 제어를 수행한다. Schema는 검증인이 증명인에게 요구하는 VC 속성을 포함하고 있으며, 증명인은 이를 기반으로 검증에 필요한 최소한의 VC 속성 정보를 조합하여 VP를 생성할 수 있다. SSIBAC은 검증인이 Schema에 PRP의 접근 제어 정책 VC를 포함하여 증명인에게 반환한다. 즉, 검증인은 Schema에 접근 제어 정책을 포함한 Challenge를 생성하며, 증명인은 이에 응답할 수 있어야 한다. 증명인은 보유한 VC의 신원 속성과 접근 제어 정책에 대한 Challenge 응

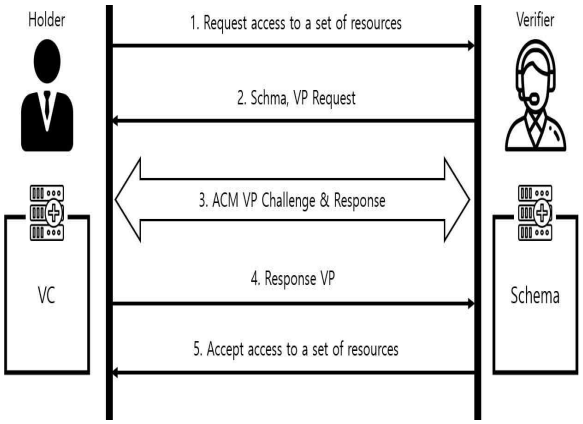

Fig 1. SSIBAC Architecture

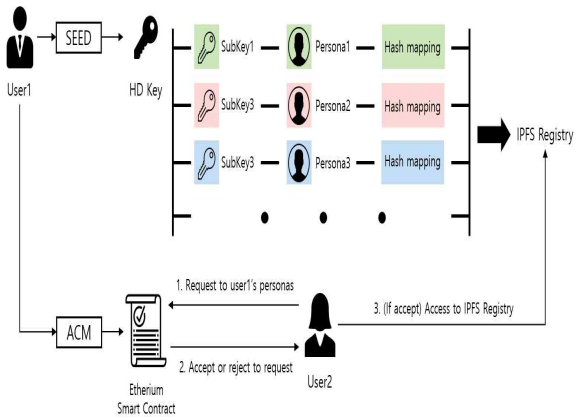

Fig 2. Jolocom ACM Architecture

답을 VP의 형태로 구성하여 검증인에게 전송하며, 검증인은 이를 검증하는 것으로 접근 권한을 부여할 수 있다.

3.3. Jolocom

Jolocom은 계층형 결정적(Hierarchial Deterministic, HD) 키 기반의 ID 관리 시스템을 제안하였다[5]. SOVRIN 등의 오픈 소스 프로젝트와 마찬가지로 정보 주체에 대한 제한적 정보 제공, 명백한 동의, 삭제권 등 강력한 자기 주권형 동작을 보장하는 것을 목표로 한다.

Jolocom은 알려진 시드(Seed)에서 생성되어 사용자에 의해 직접적으로 제어되는 HD 키를 사용한다. 이는 계층형 결정적 특성으로 인해 계층적인 복수 파생키를 생성할 수 있으며 같은 시드를 공유한다. HD 키의 각 파생키는 Jolocom 환경에서 페르소나(Personas)로 정의된 하위 ID를 생성하며, 원본 HD 키를 DID와 결합한다. 이후 파생키 및 시드를 기반으로 하여 개인의 페르소나를 식별하고, ACM을 위한 각 페르소나에 IPFS의 해시 매핑을 수행한다. 결과적으로 IPFS 구조 하에서 이더리움의 스마트 컨트랙트를 통한 접근 제어를 달성한다.

IV. 결론

본 논문은 SSI의 탈중앙형 동작 개념 하에서 ACM을 제공하기 위한 현행 연구 동향의 고찰을 진행하였다. 그 결과, SSI 솔루션의 ACM 기준이 제안되지 않았기 때문에 기존 SSI 솔루션들은 독립적인 ACM 기술을 구현하는 것으로 분석되었다. 이에 본 논문은 관련 연구 분석을 통해 탈중앙형 신원 식별 서비스 기반 안전한 접근 제어 기법에 대한 연구 시사점을 환기하였으며, 추후 다양한 관점에서의 ACM 기법 연구가 제안될 것임을 기대할 수 있다.

Acknowledgement

이 논문은 2020년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. 2019R1I1A3A01060652).

[참고문헌]

[1] D. Reed et al., “Decentralized Identifiers(DIDs) v1.0”, W3C Working Draft, (2020, Nov. 08) [Online]. Available: https://www.w3.org/TR/did-core/

[2] Roos, Julian. "Identity management on the blockchain." Network 105 (2018).

[3] S. Sandhu, E. Coyne, H. Feinstein, and C. Youman, “Role Based Access Control Models,” Computer, vol. 29, no. 2, pp. 38 - 47, 1996.

[4] Belchior, Rafael, et al. "SSIBAC: Self-Sovereign Identity Based Access Control." (2020).

[5] Fei, Ch, et al. "Jolocom: Self-sovereign and decentralised identity by design." White paper (2018).