마이데이터 플랫폼을 위한 DID 기술 단계적 적용방안 연구

박소현*, 김현준*, 이강효*, 하태균*, 김경백†
한국인터넷진흥원*, 전남대학교†
sohyeon@kisa.or.kr, hyunjun@kisa.or.kr, kanghyo.lee@kisa.or.kr, niceha@kisa.or.kr, kyungbaekkim@jnu.ac.kr

A Study on Stepwise Approach of DID Technology for MyData Platform

Sohyeon Park*, Hyunjun Kim*, Kanghyo Lee*, Tae Gyun Ha*, Kyungbaek Kim†
Korea Internet & Security Agency*, Chonnam National Univ.†

요 약

전 산업에서 데이터 가치와 효용성은 점차 높아지고, 기업들은 개인 데이터를 활용해 다양한 비즈니스로 수익을 창출하고 있다. 하지만 기업이 주도적으로 개인 데이터를 관리하고 활용함에 따라, 데이터 제공자인 정보 주체는 데이터 활용 과정에서 발생하는 혜택에서 제외되는 모순된 상황에 놓였다. 이에 정보 주체의 데이터 소유권 및 통제권 보장에 대한 필요성이 대두되면서 마이데이터(MyData) 개념이 도입되었다. 국내에서는 '20.8월 데이터3법(개인정보보호법, 신용정보법, 정보통신망법)이 통과되어 신용정보법에 본인신용정보관리업(마이데이터산업) 추진 근거가 마련되었고, 이에 따라 금융분야 마이데이터 산업이 활성화되기 시작했다. 그러나 현존하는 마이데이터 플랫폼은 중앙화된 시스템으로 본래 취지와 다르게 정보 주체의 데이터 소유권 및 통제권 등을 완벽히 보장하기에 역부족이다. 이에 본 논문에서는 기존 마이데이터 플랫폼의 한계점을 분석하고, 데이터 주권이 정보 주체에게 있고, 필요할 때 개인 데이터를 중앙화 시스템을 거치지 않고 제출·증명할 수 있는 기술인 DID(Decentralized ID) 기술의 단계적 적용방안을 제안한다.

Ⅰ. 서 론

마이데이터는 데이터 주권이라는 철학 아래 기본적으로 데이터의 소유권을 가진 정보 주체가 자신의 데이터를 직접 소유하고 통제할 수 있도록 하는 '개인정보자기결정권'과 자신의 정보를 제3자에게 전송·관리할 수 있도록 허용하는 '개인정보이동권'을 핵심으로 설계되었다. 기존의 데이터 체계는 데이터 보유기업에 종속적이어서 그 내용과 활용처에 대해 정보 주체는 알 수 없었으며, 제공된 데이터의 가치를 공유받지 못했다.

이를 보완하고자 마이데이터 체계에서는 정보 주체도 자신의 데이터에 접근 및 활용할 수 있도록 시스템을 마련하고자 하는 것이다. 국내 마이데이터의 제도적 기반은 '개인신용정보 전송요구권'(신용정보법 제33조의2)으로 정보 주체가 자신의 개인신용정보를 금융 회사로부터 마이데이터사업자에게 전송하도록 요구할 수 있는 권리를 기반으로 한다.[1]

마이데이터사업자는 이를 기반으로 은행, 카드, 보험, 증권 등에 흩어져 있는 정보 주체의 금융정보를 일괄 수집하여 정보 주체가 알기 쉽게 통합하여 제공하는 서비스를 운영하고 있다. 국내 대표적인 사례로는 뱅크샐러드와 각 은행사의 마이데이터 서비스 등이 있으며 은행, 증권을 포함한 총자산액과 보험 관련 데이터 등을 한 번에 확인할 수 있다.

그러나 현존하는 마이데이터 플랫폼은 중앙화된 플랫폼으로 본래 취지와 다르게 데이터 소유권과 통제권 등을 완벽히 보장하기에 한계가 있다. 이에 본 논문에서는 기존 마이데이터 플랫폼 한계점을 분석하고, 정보 주체의 데이터 소유권과 통제권을 온전히 보장할 수 있는 DID 기술을 마이데이터 플랫폼에 단계적으로 적용하는 방안을 제안하고자 한다.

Ⅱ. 마이데이터에 DID 기술 적용 필요성

2-1. DID 기술 개요

DID는 정보 주체의 개인 데이터에 대한 통제권을 서비스 기업에서 개인에게 돌려주어 자기 주권을 보장할 수 있다.[2] DID 체계에서 정보 주체는 개인 데이터를 자신의 휴대폰 등에 저장하고 상황에 따라 필요한 정보만 선택해 제출할 수 있다. 오프라인에서 신원확인 시 지갑에서 신분증을 꺼내 본인을 증명하는 것처럼 휴대폰 전자지갑에 담긴 개인 데이터를 전자적으로 제출하여 본인을 증명하는 것이다.

참여자는 [표 1]과 같이 발급기관, 사용자, 검증기관, 데이터레지스트리로 구분된다. 발급기관(Issuer)은 사용자(Horder)가 요청할 때 신원확인 후 보유하고 있던 사용자 개인 데이터(신원·신용정보 등)를 전자적 형태(VC)로 발급한다. 사용자는 해당 데이터(VC)를 전자지갑에 저장하고, 데이터 제공이 필요한 시점에 검증기관(Verifier)에게 제출한다. 이후 검증기관은 그 사용자의 데이터가 맞는지 검증하고 서비스를 제공하는 구조이다. 각 과정에서 생성되는 데이터는 각 주체의 개인키로 전자서명 되며, 이는 데이터레지스트리에 저장된 각 주체의 공개키로 검증할 수 있다.

[표 1] DID 체계 참여자

구분	역할
발급기관 (Issuer, 정보제공자, 데이터 보유기업)	하나 이상의 정보 주체에 대한 클레임(개인 데이터 조각)을 확증하고, 클레임으로부터 VC(개인 데이터)를 생성하는 역할 (예, 은행, 증권사 등)
사용자 (Holder, 정보주체)	하나 이상의 VC(Verifiable Credential, 개인 데이터)를 보유하고 그것으로부터 VP(Verifiable Presentation, 개인 데이터의 재조합 데이터)를 생성하는 역할
검증기관 (Verifier, 정보수신자, 데이터 이용기업)	검증 절차를 위해 하나 이상의 VC, VP를 받는 역할로 사용자에게 일정 리워드를 지급하고 정보를 제공받을 수 있음 (예, 일반기업, 마이데이터사업자 등)
데이터레지스트리 (Verifiable data registry)	신뢰할 수 있는 블록체인 플랫폼 등으로 VC 스키마, 참여자 공개키와 같은 식별자, 키 및 기타 관련 데이터의 생성, 확인을 중재하는 역할

2-2. 기존 마이데이터 플랫폼 한계점 분석

정보 주체의 적극적인 관리·통제기반의 서비스 제공을 위해 '마이데이터 플랫폼'이 등장했음에도 본래 취지와 다르게 정보 주체의 데이터 소유권과 통제권을 완벽히 보장하기에는 역부족이다.

첫째, 현재 운영되고 있는 마이데이터 플랫폼은 정보를 저장하고 관리하는 주체가 개인이 아닌 중앙화된 플랫폼이기 때문에 '개인정보의 주권을 개인이 소유하고 관리한다'라는 소유권 보장 취지에 부합하지 않는다. 또한, 전송된 개인정보의 활용 사항에 대해서도 실시간으로 정보 주체가 열람 및 조회가 불가함에 따라, 현존하는 마이데이터 체계에서는 정보 주체의 정보에 대한 완전한 소유권 보장은 어려운 상황이다. 나아가 보안 측면에서 현재 마이데이터 플랫폼은 생태계 참여기업이 많아질수록 개인정보 유출 위험이 증가하는 한계점이 존재한다.

둘째, 현재 운영되고 있는 마이데이터 플랫폼에서는 정보 주체의 실질적인 통제권 보장이 불가하다. 마이데이터의 본래 취지에 따라, 정보 주체의 통제권을 완벽히 구현하기 위해서는 정보 주체가 기업·기관에게 자신의 데이터를 직접 전송 및 회수할 수 있는 기술 확보가 선행되어야 한다. 그러나 현재는 정보 주체의 데이터 상당수를 금융 회사 등 데이터 보유기업(발급기관)이 마이데이터사업자 등(검증기관)에게 직접 전송하게 된다. 따라서, 정보 주체의 요청 사항에 따라 데이터를 전송한다 해도 데이터 수집 및 관리하는 기업이 시스템으로 송·수신을 결정할 수 있어서 악용한다면 정보 주체의 데이터를 통제할 수 있다.

2-3. DID 기술 적용시 이점

행정안전부의 모바일 공무원증·운전면허증, 질병관리청의 백신접종서비스('COOV') 등 모두 DID 기술로 개발된 만큼 기술의 안전성과 활용성은 이미 입증된 바 있다. 이에 DID 기술을 마이데이터 플랫폼에 적용한다면 안전성과 앞으로의 활용 가치를 더 높일 수 있을 것이다.

첫째, 정보 주체가 개인 데이터(VC)를 중앙화된 플랫폼이 아닌 본인 휴대폰 혹은 개인 클라우드에 저장하고 관리하기 때문에 '개인정보의 주권을 개인이 소유하고 관리한다'라는 마이데이터 취지에 부합한다. 또한, 보안 측면에서도 대규모 유출 위험성을 낮출 수 있다.

둘째, 개인 데이터 통제권을 온전히 보장할 수 있다. DID 체계에서 정보 주체는 데이터 보유기업으로부터 자신의 데이터를 받아 휴대폰 등에 보관하고 있기 때문에 보유기업에게 별도 요청 절차 없이 이용기업(검증기관)에게 언제나 데이터를 직접 제공할 수 있다. 이에 정보 주체가 어떤 이용기업에게 어떤 데이터를 제공했는지 보유기업에게 공개되지 않는다.

셋째, DID는 기본적으로 데이터 전송과정에서 각 주체의 개인키로 전자서명 된 데이터를 전송·제공하기 때문에 데이터 출처에 대한 신뢰성 보장, 데이터 위변조 방지, 제공 사실 등에 대해 부인 방지할 수 있다. 이에 문제 발생시 책임 소재를 명확히 할 수 있다.

Ⅲ. 마이데이터에 DID 기술 단계적 적용방안

현재 모든 마이데이터 플랫폼이 기업 중심에서 개인 중심으로 변화하기는 현실적으로 어려울 것이다. 이에 기존 마이데이터 플랫폼에 단계적으로 DID 기술을 적용할 수 있는 모델을 제안한다.

3-1. (모델1) 기존 마이데이터 플랫폼에 신원확인만 DID를 적용하는 모델

기존 마이데이터 플랫폼에서 정보 주체가 데이터 보유기업(발급기관)으로부터 데이터를 받아오기 위해 수행하는 신원확인 단계에만 DID를 적용하는 방식이다. 본 모델은 기존 마이데이터 플랫폼의 구현 시나리오를 최대한 반영함과 동시에 신원정보를 휴대폰에 안전하게 발급·저장·제출함으로써 신원정보 소유권과 통제권을 보장할 수 있다. 국내에는 금융결제원의 '마이인포'(전자지갑)의 '뱅크아이디' 서비스가 유사하다. '뱅크아이디'는 16개 은행이 공동으로 참여 및 발급하는 은행권 공동서비스이며, 각 은행에서 회원 가입시 반복적으로 신원정보를 입력해야 하는 번거로움을 없애주는 역할을 한다. 예를 들면 마이데이터 플랫폼에서는 이러한 '뱅크아이디'와 같은 서비스로 통합인증 후 여러 기관의 데이터를 한 번에 전송 요청받을 수 있다.

3-2. (모델2) 개인 데이터를 신뢰할 수 있는 기관에 위탁하는 모델

정보 주체가 데이터 보유기업에게 받은 개인 데이터를 본인의 휴대폰 혹은 개인 클라우드가 아닌 데이터 보관·관리에 전문성이 있는 제3자인 보관자에게 위탁하는 모델이다. 여기서 보관자는 마이데이터사업자가 되거나 보관 서비스만 제공하는 커스터디사업자가 될 수 있다. 모델1과의 차이점은 신원확인뿐 아니라 이후 단계의 마이데이터 전달체계에서도 DID가 적용되며, 데이터 보관 플랫폼은 IPFS(InterPlanetary File System, 분산형 파일시스템)을 이용한다. 정보 주체의 소유권, 통제권 보장 수준은 모델1과 비슷하지만, 분산형 시스템을 이용하기 때문에 마이데이터 유출 위험성을 낮출 수 있다. 또한, 데이터 전송 이력들은 별도의 블록체인에 기록하여 투명하게 관리할 수 있다.

3-3. (모델3) 개인 데이터를 온전히 정보 주체가 관리하는 모델

마이데이터사업자 등 중앙, 분산된 플랫폼 없이 정보 주체가 온전히 개인의 정보를 휴대폰, 개인 클라우드, PDS(Personal Data Store, 개인 데이터 저장소)를 이용해 저장·관리·전달할 수 있는 모델이다. 정보 주체의 소유권과 통제권 보장 수준이 가장 높다. 정보 주체는 전자지갑으로 언제나 데이터 이용기관에게 데이터를 직접 제출하고 제출된 이력을 관리 할 수 있다.

Ⅲ. 결론

현재 마이데이터 서비스에서 정보 주체는 데이터를 편리하게 통합·조회할 수 있는 서비스를 이용할 수 있다는 이점 하나로 데이터 가치를 넘기고 있다. 하지만 실제로 기업들은 이 데이터를 통해 또 다른 비즈니스 모델을 창출하고 있다. 기업이 이미 보유하고 있는 데이터에 대한 가치를 보장받을 수는 없지만, 데이터의 가치가 점차 커지고 있는 만큼 앞으로 계속 생성될 데이터의 가치는 보존 받을 수 있어야 한다.

본 논문에서는 정보 주체가 개인 데이터에 대한 소유권 및 통제권을 온전히 보장받고, 데이터 활용에 대한 가치 혜택을 받을 수 있도록 기존 마이데이터 플랫폼에 DID 기술을 단계적으로 적용할 수 있는 방안을 제안했다. 향후 연구에서는 각 모델을 구체화하고, 정보 주체의 혜택을 중심으로 금융뿐 아니라 의료, 공공, 웹3 서비스 등에 적용할 수 있는 모델을 분석하고자 한다.

참 고 문 헌

[1] 마이데이터 종합포털
(https://mydatacenter.or.kr:3441/myd/index/index.do)

[2] J. Lee, K. Lee, and K. Kwon, "Current status of blockchain-based decentralized ID ecosystem and policy suggestions," in Proc. KICS Winter Conf. 2020., pp. 1048-1049, YongPyung Resort, Korea, Feb. 2020