Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.3, Jun. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.3.513

분산 ID 보관 및 연계 서비스 모델 제안*

여 기 호,[1†] 박 근 덕,[2] 염 흥 열[3‡]
[1,3]순천향대학교 (대학원생, 교수), [2]서울외국어대학원대학교 (교수)

Proposal for a Custody and Federated Service Model for the Decentralized Identity*

Kiho Yeo,[1†] Keundug Park,[2] Heung Youl Youm[3‡]
[1,3]Soonchunhyang University (Graduate student, Professor),
[2]Seoul University of Foreign Studies (Professor)

요 약

오늘날까지 정보주체의 개인정보들은 많은 기업이나 기관에 중앙 집중화되어 있는 구조였다. 하지만, 최근에는 점차적으로 정보주체가 자신의 개인정보를 통제하고 소유권을 찾는 방향으로 패러다임이 변화하고 있다. 해외는 일찍부터 EU의 일반 개인정보보호법(General Data Protection Regulation)이나 미국의 소비자 프라이버시 권리장전(California Consumer Privacy Act) 등으로 개인의 데이터 소유권을 강화하고 있다. 국내도 여러 기업들이 모인 연합체들에 의해 분산 ID 서비스 모델에 대한 기술 연구와 서비스 적용 사례들을 만들어 가고 있다. 본 논문에서는 현재 연구되고 있는 분산 ID 서비스 모델과 그 한계점에 대해 알아보고 해결할 수 있는 보다 개선된 분산 ID 서비스 모델을 제안하고자 한다. 제안 모델은 분산 ID를 제3의 기관인 보관자에게 안전하게 수탁하는 기능과 서로 다른 분산 ID 서비스가 생기더라도 상호 연동될 수 있는 연계 기능을 가진다. 아울러, 제안 모델의 보안 위협을 식별하고 보안 요구사항을 도출하여 보다 안전하고 편리한 모델을 제시한다. 분산 ID 기술은 사람에 대한 증명뿐 아니라 향후 사물인터넷의 디바이스 ID 인증 관리에도 확장되어 적용될 것으로 기대된다.

ABSTRACT

Until today, the personal information of subjects has been centralized in many companies or institutions. However, in recent days, the paradigm has gradually changed in the direction that subjects control their personal information and persue their self-sovereignty. Globally, individual data sovereignty is strengthened by the European Union's General Data Protection Regulation(GDPR) and the US California Consumer Privacy Act(CCPA). In Korea, a few alliances consist of various companies are creating technology research and service application cases for decentralized ID service model. In this paper, the current decentralized ID service model and its limitations are studied, and a improved decentralized ID service model that can solve them is proposed. The proposed model has a function of securely storing decentralized ID to the third party and a linkage function that can be interoperated even if different decentralized ID services are generated. In addition, a more secure and convenient model by identifying the security threats of the proposed model and deriving the security requirements, is proposed. It is expected that the decentralized ID technology will be applied not only to the proof of people but also to the device ID authentication management of the IoT in the future.

Keywords: Distributed Ledger Technology, Decentralized Identity, Self Sovereign Identity, Custody, Federation

Received(03. 16. 2020), Modified(06. 03. 2020), Accepted(06. 03. 2020)

* 본 논문은 과학기술정보통신부와 정보통신기획평가원이 지원하는 '차세대 ICT 환경에서의 보안 및 개인정보보호 기술 국제 표준화 추진' 사업(과제번호: 2019-0-00660)의 지원 및 2017년도 순천향대학교 교수연구년제의 연구에 의하여 수행되었습니다.

† 주저자, symbol.yeo@hyundai-autoever.com
‡ 교신저자, hyyoum@sch.ac.kr(Corresponding author)

I. 서 론

전통적으로 사람이 사회·경제 활동을 하기 위해서는 "내가 누구인지"를 증명할 수 있는 수단이 필요했다. 인터넷의 등장 이후, 디지털 시대에서 디지털 ID를 사용하게 되면서 자기를 증명하기 위한 많은 방법들이 시도 되고 있다. 사람을 인증하는 대표적인 방법으로 지식기반, 소유기반, 생체기반 방식[1]들이 있다. 국내에서는 금융 및 공공 서비스 등과 같은 중요한 서비스를 이용하기 위해서는 제3의 신뢰된 기관으로부터 발급받은 공인인증서를 이용하는 PKI 기반의 인증 방식이 널리 사용되어 왔다. 하지만, 공인인증서는 발급, 갱신 등의 관리하는 절차가 복잡하고 불편함이 존재한다. 또한 서비스를 제공받기 위해 기업이나 기관이 추가적인 개인정보를 수집하고 이용할 권한을 동의해야 하고, 서비스의 종류에 따라 요구되는 보증수준(level of assurance)[2]이 다름에도 불구하고 과도하게 정보가 제공되어, 자신의 개인정보에 대한 통제력을 상실하게 된다. 설상가상으로 개인정보를 저장하고 있는 그 기관이나 기업이 부주의나 고의, 오류 등으로 안전하게 관리하지 못한 경우, 개인정보 유출의 1차적인 피해는 고스란히 개인의 몫이 된다.

이러한 문제점들을 개선하기 위해, 2016년 크리스토퍼 알렌(christopher allen)이 자기주권 신원증명(self sovereign identity)의 개념에 대해 언급한 뒤로 W3C를 중심으로 다양한 연구를 진행해 왔다[3]. 자기주권 신원증명은 사용자 중심의 신원증명을 넘어 사용자 스스로가 신원증명 정보를 관리하고 통제하는 개념이다. 그리고 최근에는 분산원장기술(DLT : Distributed Ledger Technology)을 접목하여 신뢰 기반의 신원증명 발급과 검증이 가능한 분산 ID(decentralized IDentity) 모델을 발전시켜 다양한 서비스 사례에 적용하기 위한 연구가 활발하게 진행 중이다. 여기서 분산 ID는 디지털 환경에서 정보주체가 스스로 신원정보의 관리, 제출 범위 및 대상 통제 등을 통해 자기주권을 보장할 수 있는 탈중앙화된 디지털 신원증명 체계를 의미한다[4]. 현재까지 논의되고 있는 분산 ID 서비스 모델의 문제는 사용자의 모바일 기기에 신원정보와 개인키를 저장하는 방식이기 때문에, 모바일 기기 사용에 대한 문제점을 그대로 가지게 된다. 또한 이기종 분산 ID간의 상호연동 이슈도 언젠가는 다루어야 할 문제로 남아 있다. 이러한 문제점들을 해결하기 위해서는 보다 개선된 서비스 모델이 필요하다고 판단되어, 분산원장기술 기반의 분산 ID를 안전하게 보관하는 수탁 서비스 모델을 제안한다.

따라서, 본 논문의 제2장에서는 분산 ID와 관련된 국내외 연구 동향과 그 공통 모델에 대해 알아보고, 제3장에서는 기존 분산 ID 서비스 모델의 한계점에 대해 설명한다. 제4장에서는 기존 모델의 문제점을 해결한 새로운 분산 ID 보관 및 연계 서비스 모델을 제안하고 개선된 모델의 보안 요구사항과 그 기대효과를 짚어보기로 한다. 마지막으로 제5장에서는 결론 및 향후 발전 방향에 대해 설명한다.

II. 관련 연구 및 기존 모델

2.1 해외 사례

분산원장기술을 활용한 분산 ID 기술은 아직 진행 과정에 있는 미완성 상태이지만, 기술 개발 및 표준화를 위해 많은 글로벌 기업들이 참여하면서 빠르게 발전할 것으로 예상된다. 해외에서는 마이크로소프트나 IBM과 같은 단일 글로벌 기업을 중심으로 연구를 진행하거나, 여러 기업 또는 기관이 연합으로 공동 연구를 진행하고 경우가 있다. 본 논문에서는 다양한 이해관계자들의 참여를 통해 분산원장기술 기반의 분산 ID를 연구하는 기구나 단체의 사례를 알아본다. 대표적으로 분산식별자 및 신원 증명서 표준화를 주도하는 W3C (World Wide Web Consortium)[5], 분산 ID의 상호연동 및 기술개발을 위한 산업체 연합인 DIF (Decentralized Identity Foundation)[6], 디지털 자기주도 신원증명 오픈소스 프로젝트에 대한 기술 지원을 제공하는 비영리 단체 SOVRIN Foundation[7]이 있다.

① W3C

1994년 설립된 W3C는 웹 기반의 기술 표준화를 추진하는 기구이다. Fig.1.에서 보는 바와 같이 분산 ID를 구성하는 발급기관(Issuer), 정보주체(Holder), 검증기관(Verifier)의 역할과, 신원증명서 (Verifiable Credential, VC), 분산식별자(Decentralized Identifier, DID), DID문서(DID Document)와 같은 정보들을 표준화 하고 있다. W3C에서는 분산 ID(DID)를 분산화된 신원(Decentralized Identity)이 아닌 분산식별자(Decentralized Identifier, DID)로 정의하고 ,

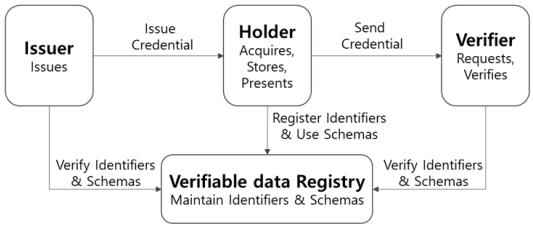

Fig. 1. Basic DID Model of W3C [12]

RFC4122[8]에 명시된 UUID(Universally Unique Identifier)와 유사한 텍스트 문자열로 설명하고 있다[9].

W3C의 분산 ID 서비스 모델은 증명서 기반의 모델로써 본인 정보가 포함된 신원증명서를 발급받아 정보주체가 전자지갑에 보관, 관리하며, 필요시 본인이 직접 제출하는 방식이다. 이때, 분산원장기술은 분산식별자 저장소(DID registry)의 역할을 하며, 신원 증명서의 유효성을 검증할 수 있도록 지원한다[10][11].

② DIF

2017년 설립된 DIF는 분산 ID 생태계를 구축하고자 마이크로소프트, IBM, 마스터 카드를 비롯한 80여개 기업이 모여 만든 표준기술 개발기구이다[6]. 또한, 개방적인 생태계를 구축하기 위해 모든 참가자들 간 상호연동 및 연계기술을 개발하는 엔지니어링기반 조직이다[11]. DIF 워킹그룹에서는 분산 ID 기반 인증(DIDauth)과 관련된 사양, 표준, 라이브러리를 설계 및 구현하고, 인증된 메시지 기반 통신(DIDComm)을 위한 사양을 구현하여 오픈소스로 기증을 한다[6]. 분산 ID의 기반기술은 W3C와 DIF를 중심으로 표준화가 진행 중이다[4].

③ SOVRIN Foundation

2016년에 설립된 SOVRIN 재단은 각국의 기업 또는 개인이 참여하고 있는 비영리 단체이다. SOVRIN 재단은 분산 ID 연합 생태계 구성에 가장 적극적인 단체로 분산 ID 전용 블록체인 네트워크를 구축하고 상용서비스도 개시하였다. SOVRIN 재단이 W3C와 다른 점은 Fig.2.에서 보는 바와 같이 검증 가능한 신원증명 과정에서 발급기관, 정보주체, 검증기관 간에 유일한 분산 ID를 사용한다는 것이다[11]. SOVRIN 재단 소속의 DID 전문 기업인 Evernym은 분산ID 전용 블록체인 플랫폼인 하이

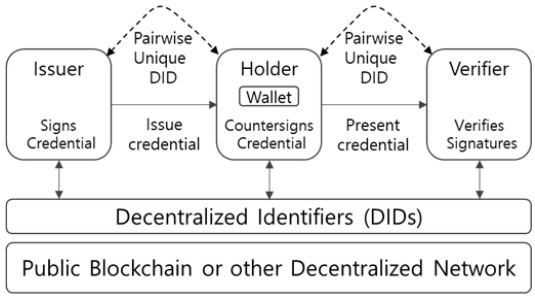

Fig. 2. Decentralized ID Model of SOVRIN [13]

퍼레저 인디(Hyperledger Indy) 개발에 참여하여 오픈소스로 무상 기증하기도 하였다[14].

2.2 국내 사례

국내 분산 ID 연구 방향은 처음부터 여러 기관들이 컨소시엄이나 얼라이언스 형태로 세력을 형성하여 분산 ID 적용 생태계를 조성하고, 실제 적용 가능한 서비스 발굴에 집중하고 있다. 또한, 공통적으로 W3C의 표준을 준용하고 있지만, 서로 다른 연합체에서 기술 표준을 조금씩 다르게 발전시키고 있다. 이러한 문제점을 해소하기 위해 한국인터넷진흥원과 금융보안원에서 향후 분산 ID 생태계 확산을 위한 가이드라인을 마련하고, 분산 ID 관련 정책·기술 연구 및 표준화 추진 등을 위한 업무 협약을 맺기도 하였다[15]. 현재 국내에서 현재 분산 ID 생태계를 만들고 있는 단체는 3군데가 있다. 금융과 통신, IT, 전자 분야의 대형 기업들이 포함되어 있는 Initial DID Association[16], 금융결제원, FIDO Alliance와 함께 다양한 기업들이 모여 가장 먼저 출범한 DID Alliance Korea[17], 암호 화폐 ICO 경험과 분산원장 플랫폼을 개발한 전문업체 위주로 연합이 구성된 MyID Alliance[18]등이 존재한다.

① Initial DID Association

2019년 설립된 이니셜 DID 연합은 국내 통신 3사, 주요 은행 5개, 신용카드사 2개, IT회사 및 삼성전자 등 현재 14개 기업이 컨소시엄에 참여하고 있다. 과학기술정보통신부와 한국인터넷진흥원이 주관하는 '2019 블록체인 민간주도 국민 프로젝트'를 계기로 SKT 중심으로 결성된 컨소시엄이 국민이 편리하고 안전하게 이용할 수 있는 모바일 전자증명 시

범서비스를 추진하고 있다[16]. 이니셜 DID 연합은 하이퍼레저 패브릭(Hyperledger Fabric) 기반으로 컨소시엄 참여사들이 Peer 운영사로 참여하기로 되어 있다. W3C의 표준기술을 적용하여 신원증명서 기반의 서비스를 개발하고 있고, 전자지갑 및 SDK는 하이퍼레저 인디의 오픈 소스를 이용한다. 2020년 초에 출시하는 이니셜(initial)이라는 모바일 앱을 통해서 정보주체가 신원증명서를 보관, 통제할 수 있다.

② DID Alliance Korea

2019년 7월 라온시큐어를 중심으로 금융결제원과 함께 국내외 56개 기업으로 구성된 연합체로, 글로벌 기술표준 수립 및 비즈니스 모델을 활발하게 연구하고 있다. 최근에는 미국에 글로벌 DID Alliance를 설립하여 국제적인 기업 연합체로 세력을 확장하고 있다[17]. DID 얼라이언스를 주도하는 라온시큐어는 블록체인 기반 개인정보 서비스인 인포월렛(infowallet) 개발을 시작으로 EOS 기반의 분산 ID 플랫폼인 옴니원(OmniOne)을 통해 기본적으로 FIDO 생체인증과 신원증명 서비스가 가능하다[19]. 실제로 라온시큐어는 옴니원 플랫폼으로 과학기술정보통신부와 한국인터넷진흥원이 주관한 '2019 블록체인 공공 시범사업'에 참여하여 새롭게 구축된 병무청 민원 포털 사이트에 분산 ID를 이용한 간편인증 서비스를 적용하였다. Fig.3.은 병무청과 국가보훈처가 연계하여 분산 ID를 이용한 서비스 구성도이다. 간편 인증 모바일 앱만 설치하면, 분산 ID로 공인인증서를 대체하여 로그인과 신원확인을 간편하게 할 수 있게 되었다. 간편 인증 서비스 후에는 병적 증명서 발급 서비스로도 확대 지원할 예정이다[20]. 한국 FIDO 산업포럼과 FIDO Alliance 창립자인 라메시 케사누팔리(Ramesh Kesanupalli)가 참여하고 있어 FIDO 생체인증 기술을 적극적으로 활용한다.

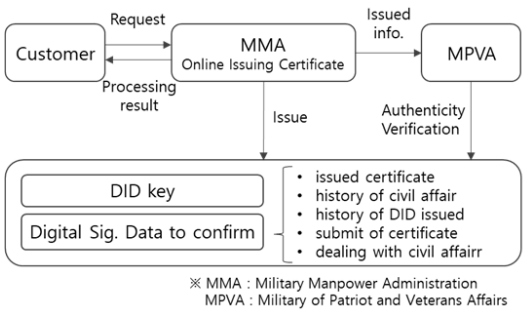

Fig. 3. Decentralized ID Service Model for Easy Authentication of MMA [20]

③ MyID Alliance

2019년 11월 출범한 MyID Alliance는 국내 분산원장기술 솔루션 기업인 아이콘루프를 중심으로 금융 또는 비금융권 분야의 52개사로 구성되어 있다. 아이콘루프의 MyID 플랫폼은 통장 개설시 비대면 인증 서비스에 대해 금융위원회의 혁신금융서비스 금융규제 샌드박스로 지정되어 있다[16]. 또한 DPASS (Decentralized PASSport)라는 분산원장기술을 이용한 신원 확인 및 암호 화폐 전자지갑(e-wallet) 기능을 가진 모바일 앱을 통해 정보 주체가 자신의 개인 정보를 안전하게 관리하고 사용할 수 있도록 제공한다. DPASS 역시 W3C의 분산 ID 표준 체계를 준용하고 있어 서비스 확장 가능성이 높다[21].

2.3 기존 분산 ID 서비스 모델

앞에서 살펴본 바와 같이 현재의 분산 ID 기술 표준은 주로 W3C나 DIF에 의해 개발되어 왔다. Fig.4.는 W3C를 비롯한 국내외 분산 ID 서비스 모델의 공통적인 부분을 도식화하였고, 각 개체들의 역할 및 서비스 흐름을 보다 상세히 설명하였다. 이 기본 모델을 기준으로 보다 개선된 제안 모델과의 차이점을 쉽게 파악할 수 있다. 기본 모델은 정보주체가 검증기관으로부터 원하는 서비스를 제공받기 위해 필요한 신원정보를 발급기관으로부터 발급 받아 제출한다. 이때 발급기관이 발행한 신원 정보의 유효성을 보장하기 위해 발급기관의 인증서를 신뢰된 저장소에 저장해 놓는다. 신원 정보를 제출 받은 검증기관은 신뢰된 저장소에서 그 유효성을 검증하고 서비스를 제공하게 된다[4].

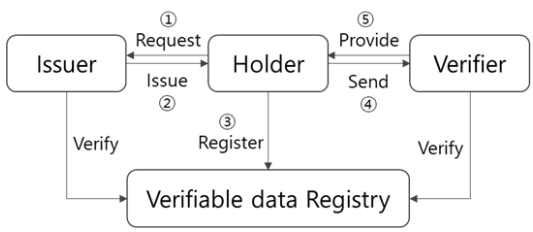

Fig. 4. Basic Model of Decentralized ID

- 발급기관(Issuer) : 정보주체의 신원정보를 보유하고 있어 정보주체의 요구에 의해 분산 ID를 발급하는 사업자 또는 기관으로 발급한 정보에 대해 신뢰할 수 있도록 인증서를 함께 전달
- 정보주체(Holder) : 분산 ID를 활용하여 본인의 신원을 증명하고자 하는 사용자로 시스템 구성에서는 분산 ID를 발급받고, 제출하는 사용자의 모바일 기기에 해당.
- 검증기관(Verifier) : 정보주체의 요구에 의해 분산 ID로 신원을 확인한 후 서비스를 제공하는 사업자 또는 기관으로 발급기관이 .발급한 유효한 신원정보라는 것을 검증 데이터 저장소를 통해 검증
- 검증 데이터 저장소(Verifiable data Registry) : 정보주체의 식별자와 발급기관의 인증서, 신원증명 해지 내역, 신원증명 스키마 등이 등록되어 있는 분산원장 기반의 신뢰된 저장소[12]

III. 기존 모델의 한계

3.1 정보주체(이용자) 보호 미흡

기존 모델의 문제점은 정보주체가 모바일 기기를 사용함으로써 발생하는 이용자 정보보호의 문제와 이용자의 편리성 저하 문제, 그리고 공통 기술 표준의 발전 미흡으로 각자 구축하는 분산 ID 체계의 상호 연동성에 관한 문제로 구분할 수 있다[4].

현재 여러 연합체에서 개발 중인 분산 ID 서비스 모델은 정보 주체가 본인의 신원 정보를 모바일 기기에 보관하도록 하고 있다. 모바일 기기를 사용하는 환경에서의 보안 위협은 디바이스, 네트워크, 플랫폼, 어플리케이션의 영역으로 나눌 수 있다. 그 중에 모바일 기기 자체에 대한 위협은 디바이스 영역으로 악성코드 감염, 분실 및 도난, 데이터 노출이 해당된다[22]. 이렇게 모바일 기기 자체가 가지는 보안 위협으로 인해 다음과 같은 해킹 및 분실(도난)로 인한 문제가 발생할 수 있다.

- 개인의 보안 수준에 따라 다르겠지만, 대부분의 모바일 이용자들이 보안에 익숙하지 않아 취약한 모바일 기기에 악성코드 또는 해킹에 의해 분산 ID 및 개인키 유출(CT1)
- 연평균 100만대 이상의 스마트 폰 분실이 발생하는 환경에서 이용자들의 모바일 기기 분실(도난)로 인한 분산 ID 및 개인키 유출(CT2)

실제로 국내외에서 모바일에 탑재되는 운전면허증이나 기업의 모바일 직원증 사용 중에 모바일 기기를 분실한다면, 신분증을 분실한 것과 동일한 피해 사례가 발생할 수 있다. 모바일 기기의 해킹이나 분실은 지갑을 분실한 것과 동일한 심각한 문제이다.

3.2 정보주체(이용자) 편리성 미흡

모바일 기기의 대중화로 대부분의 사람들이 모바일 기기 이용자이므로 분산 ID 서비스 모델에서도 보다 편리하게 분산 ID를 발급받고 정보주체의 판단에 의해 제출할 수 있도록 모바일 기기를 활용하고 있다. 하지만, 모바일 기기의 분실이나 도난으로 정보주체의 수중에 없을 경우에는 오히려 모바일 기기라는 제약으로 인해 다음과 같은 불편함이 존재한다.

- 모바일 기기라는 제한된 단말기를 사용하여 분산 ID 서비스를 이용시 모바일 기기가 수중에 없을 경우 발생하는 불편함(CT3)
- 이용자가 모바일 기기의 분실 또는 교체, 최악의 경우 분산 ID 및 개인키 유출시, 발급기관으로부터 발급받은 ID의 수만큼 폐지 및 재발급 받아야 하는 불편함(CT4)

이러한 불편함은 앞서 언급한 해킹이나 분실로 인한 유출에 비해 큰 문제가 되지 않겠지만, 서비스 활용 수단을 다양화할 필요가 있다.

3.3 상호 연동성 문제

앞서 기술했듯이, 국내 3개의 분산 ID 연합체도 DIF나 W3C의 표준을 참고하고 있으나, 아직은 표준을 모든 서비스에 적용할 수 있는 수준은 아니다. 국내의 경우도 표준화 작업이 부진하다 보니 무엇보다도 기술 표준화가 시급하게 필요하다는 지적이 나오고 있다. 공통된 기술 표준이 없거나 상세화 되어 있지 않은 상황에서는 실제로 서비스에 적용할 때는 각 기업이나 연합체마다 각자의 기술을 적용하여 조금씩 다르게 발전시키고 있어 결국 서로 다른 분산 ID 플랫폼을 구축할 수밖에 없게 된다. 최악의 경우에는 각 서비스별로 모바일 신분증을 각각 다르게 발급하여 정보주체를 매우 불편하게 만들게 되는 문제가 발생할 수도 있다.

• 분산 ID 기술을 가진 기업이나 연합체 별로 다르게 구현함으로 향후 발생할 수 있는 분산 ID 서비스 플랫폼의 상호 연동성 문제 (CT5)

IV. 분산 ID 보관 및 연계 서비스 모델 제안

본 장에서는 정보주체의 모바일 기기에 보관된 신원 정보를 보관하고, 모바일 기기 분실 및 모바일 기기 자체의 한계로 인한 문제점을 개선할 수 있는 "분산 ID 보관 및 연계 서비스 모델"을 제안하고자 한다. 이 모델은 기존의 PKI 기반 인증체계나 분산 ID 체계를 모두 개선할 수도 있고, 분산 ID 서비스 모델을 개발하는 여러 연합체간 호환성 문제나 나아가 다양한 도메인에서 독립적으로 구축되는 분산 ID 체계의 연계(federation) 이슈도 해결이 가능하다.

4.1 제안 모델

본 논문에서 제안하는 모델은 정보주체가 발급기관으로부터 발급 받는 신원 정보를 보관자가 전달 받아 안전하게 보관하고 ID 거래에 이용하게 해주는 일종의 수탁 대행 서비스이다. 제안 모델이 기존 모델의 구성요소와 다른 점은 다음 세 가지이다.

① 보관자, 통제자 추가
② ID 공유 원장과 ID 거래 원장과 같은 분산원장기술 기반의 시스템 추가
③ 검증기관이 하던 검증과 서비스 제공의 역할이 검증대행자(Verifying Agency)와 서비스 제공자(Service Provider)로 분리.

Fig.5.와 같이 제안 모델에서 새롭게 등장하는 구성요소와 용어는 다음과 같다. 여기서 Fig.4.의 기존 모델 구성요소와 중복된 설명은 제외한다.

• 보관자(Custodian) : 발급기관에 의해 발급된 분산 ID를 안전하게 보관하고 ID를 거래하는 모든 행위를 기록하는 사업자 또는 기관
• 통제자(Auditor) : 분산 ID의 보관 및 거래에 대한 정책 관리와 모니터링 및 감사를 수행하는 사업자 또는 기관
• 서비스제공자(Service Provider) : 기본 모델의 검증기관의 역할 중 정보주체로부터 분산 ID를 제출받아 정보주체의 신원이 확인되면 서비스를 제공하는 역할을 하는 사업자 또는 기관. 이때 정보주체로부터 받는 정보는 실제 신원정보가 아닌 신원을 확인할 수 있는 일종의 인증서(F-ID)이므로 기본 모델의 발급기관처럼 검증 역할은 없이 검증 후, 서비스 제공 역할만 하게 됨
(Service Provider = Relying Party)
• 검증대행자(Verifying Agency) : 기본 모델의 검증기관의 역할 중 정보주체의 분산 ID를 검증하는 사업자 또는 기관으로 보관자의 요청으로 검증 작업을 대행. 보관자가 검증대행자의 역할을 수행할 수도 있음
• ID 공유 원장(Ledger for ID sharing) : 발급기관에 의해 발급된 정보주체의 분산 ID에 매핑되는 F-ID를 보관하는 분산공유원장
• ID 거래 원장(Ledger for ID transaction) : 분산 ID의 거래시 발생하는 모든 작업 내역을 기록하고 보관하는 분산공유원장
• ID 거래(ID transaction) : 정보주체의 신원증명을 위하여 보관자와 다른 개체들 간에 수행하는 일련의 행위로써 분산 ID 발급, 등록, 이용, 조회, 갱신, 폐기 등이 해당
• F-ID(Federation-ID) : 보관자가 ID 거래를 목적으로 정보주체에게 발행하는 인증서로 발급기관에 의해 발급된 분산 ID에 매핑되어 있고, 개인정보를 포함하지 않음

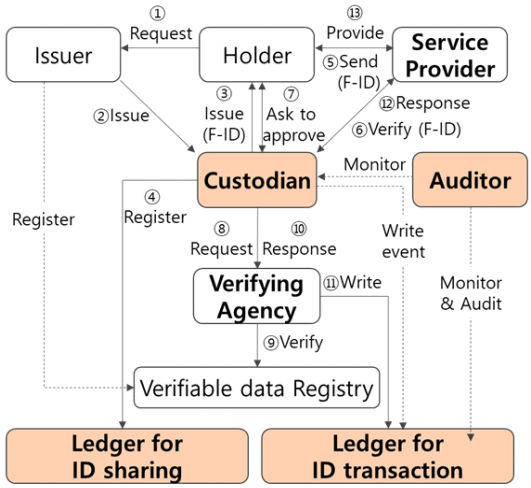

Fig. 5. Proposed Custody and Federated Service Model for Decentralized ID

Fig.5.에서 보는 바와 같이 ① 정보주체가 발급기관으로 신원 정보를 요청하면 ② 발급기관은 보관자

에게 신원 정보를 전달하여 보관자가 안전하게 보관한다. ③ 보관자는 정보주체의 실제 신원 정보 대신에 F-ID (Federation ID)라는 일종의 인증서를 정보주체에게 전달하는데, ④ F-ID는 ID 공유 원장에 기록된다. ⑤ 정보주체가 서비스를 요청하기 위해 F-ID를 서비스 제공자에게 제출하면, ⑥ 서비스 제공자는 F-ID를 발급한 보관자에게 검증을 요청하게 된다. 서비스 제공자 ⑦ 이 시점에서 보관자는 반드시 정보주체에게 검증에 대한 승인 요청을 하여, 정보주체가 승인을 했을 경우에만 검증 작업에 착수한다. 이렇게 함으로써, 정보주체는 자기주권 신원증명(SSI : Self Sovereign Identity)을 실현할 수가 있다. ⑧ 신원 검증 작업은 보관자가 검증대행자에게 요청하면, ⑨ 검증대행자가 검증 데이터 저장소를 통해 검증작업을 수행하고 ⑩ 그 결과를 보관자에게 응답한다. 이때, 검증대행자가 발급기관이 발급한 분산 ID에 대해 검증 작업을 수행하려면 사전에 발급기관의 인증서가 검증 데이터 저장소에 등록이 되어 있어야 한다. ⑪ 이러한 검증대행자나 보관자의 모든 ID 거래 이벤트 내역은 ID 거래 원장에 기록된다. ⑫ 검증 작업이 완료되었으면 보관자는 서비스 제공자에게 검증이 정상적으로 완료되었음을 응답하고, ⑬ 서비스 제공자는 정보주체가 요청한 서비스를 제공하게 된다. 마지막으로 보관자나 검증대행자가 그 기능과 역할을 제대로 수행하는지 통제자에 의해 상시 모니터링 및 정기 감사가 이루어진다.

4.2 제안 모델의 확장

국내의 경우를 보면, 여러 기업들이 모인 3군데 연합을 중심으로 분산 ID 서비스 모델이 구축되고 있다. 이렇게 분산 ID 서비스 모델을 실제로 비즈니스에 적용하다 보면, 사회적 합의를 이루어 여러 도메인에 걸쳐 통합 분산 ID 플랫폼을 만들어 사용하기가 쉽지 않다. 개별적으로 구축된 서비스들끼리 ID 연계가 필요하게 되면, 필요한 서비스마다, 또는 도메인마다 연계를 해야 하는 비용이 발생한다. 이와 같이 여러 도메인에 걸쳐 각기 다르게 분산 ID 서비스 모델이 구축될 경우에도 새롭게 제안된 모델을 적용하면, 보관자들이 공통된 ID 공유 원장에 접근하여 도메인간 연계를 제공하는 서비스 모델로도 확장이 가능하다. 여기서 ID 거래에 참여하는 모든 개체들이 ID를 통합 관리하는 것이 아니라, Fig.6.과 같이 제안된 분산 ID 서비스 모델에 새롭게 추가되는 보관자들끼리 합의가 되어, 보관자들만 참여하는 분산원장 기반의 ID 공유 원장을 구축하면, 보관자들에게 분산 보관하면서 도메인간 ID 연계도 가능하다.

ID 공유 원장 없이 도메인간 ID 연계를 할 경우, 각 도메인별로 모두 연합을 구성하여야 하는 복잡한 절차와 비용을 감소시킬 수 있고, 이러한 도메인이 더 많아질수록 정보주체들은 폭넓은 서비스를 편리하게 누릴 수 있게 될 것이다.

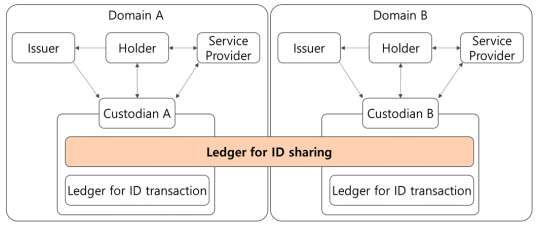

Fig. 6. Extended Custody and Federated Service Model for Decentralized ID

4.3 보안 요구사항 적용

4.3.1 제안 모델의 보안 위협

제안 모델에 추가된 보관자에게는 보관과 연계를 위한 서비스 기능도 중요하지만, ID 거래를 위한 보안이 가장 중요한 요소가 될 것으로 판단된다. 제안 모델에 대한 보안 위협은 기존의 IT 서비스에서의 일반적으로 발생하는 위협보다는 분산원장기술 기반의 ID 거래 서비스에 초점을 맞추어 결과적 위험 수준을 고려해 다음과 같이 식별하였다[23].

- ID 유출(ST1) : 외부 해킹에 의해 보관자가 보관하고 있는 정보주체의 분산 ID가 유출될 수 있다.
- ID 무단 도용(ST2) : 보관자의 내부자에 의해 정보주체의 분산 ID를 무단으로 도용할 수 있다.
- ID 거래 내역 위·변조(ST3) : 보관자는 분산 ID의 거래 내역을 위·변조 할 수 있다. 제안 모델에서는 ID 거래와 관련된 모든 이벤트 내역이 통제자에 의해 모니터링 및 감사 대상이 되므로 ID 유출 및 무단 도용시 해당 기록을 훼손하려 할 수 있다.
- 암호키 유출(ST4) : 보관자가 분산 ID를 안전하게 거래 및 보관하기 위해 생성한 암호키가

외부에 유출될 수 있다. 전자서명 및 중요 데이터 암호화에 사용되는 암호키가 유출되면 2차 피해로 확대될 수 있다.

- 어플리케이션 위·변조(ST5) : 분산원장에 기록된 정보는 위·변조가 어렵지만, 이전에 정보를 처리하는 시스템이나 각 노드에 있는 어플리케이션이 악의적으로 변경되거나 악성코드에 감염되면, 서비스 지연이나 중단이 될 수 있다.
- 비인가 접근(ST6) : 보관자가 운영하는 분산원장이나 ID 보관 및 거래 시스템에 비인가 접근이 허용될 경우 서비스 중단 및 이용자의 손실이 발생할 수 있다.

현재 도출된 위협 외에도 다른 위협이 존재할 수 있으나, 분산원장기술이 적용된 시스템을 기준으로 주로 식별되는 위협을 제시하였다. 앞으로 해킹 기술 발전으로 새로운 위협이 얼마든지 나타날 수 있고, 그러한 위협은 추후 연구항목이 될 수 있다.

4.3.2 제안 모델이 갖추어야 할 보안 요구사항

보관자가 추가된 수탁 서비스 모델에 대한 보안 요구사항은 정보통신단체표준(표준번호 : TTAK.KO-12.0352)[24] '분산원장기술 기반의 디지털 자산 거래 서비스 모델 보안 요구사항'에 기술되어 있는 내용에 기초하고 있다. 이 표준은 금융에서 사용되는 분산원장 기술 기반의 디지털 자산, 즉 암호 화폐와 같은 거래 수단을 취급하는 서비스 모델에 대해 기술되어 있지만, 분산 ID와 같은 디지털 신원정보를 디지털 자산으로 보면 매우 유사한 서비스 모델이다. 이 표준에서 다루는 8가지 보안 요구사항은 이용자 식별 및 인증, 네트워크 분리, 악성코드 통제, 데이터 암호화, 데이터 무결성, 암호키 생성 및 이용, 로그 기록 및 보존, 비정상 거래 탐지 시스템 운영으로 정보보호 및 개인정보보호 관리체계(ISMS-P)의 보호대책을 분석하여 제시한 것이다.[24]. 이 중에서 이용자 식별 및 인증 항목은 정보주체의 영역으로 모바일 앱에서 사용자를 인증하고, 발급기관으로부터 신원 정보를 발급받기 전에 수행하는 본인확인 절차로 제안 모델에서는 제외한다. 여기서는 기존 모델과 다른 보관자와 통제자를 중심으로 보안 요구사항을 기술한다.

① 네트워크 분리 : 보관자는 중요 자산(분산 ID, 암호키, ID 공유 원장, ID 거래 원장 등)의 악의적

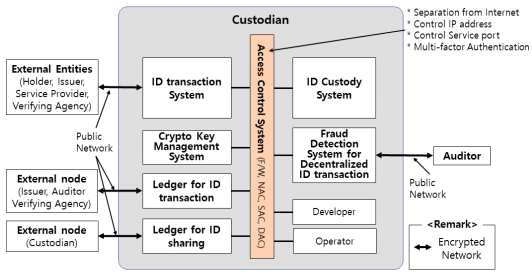

Fig. 7. Security Requirement for Network Separation [24]

공격으로 인한 유출 방지를 위해 물리적 또는 논리적으로 네트워크를 분리하여 접근 통제를 강화해야 한다. Fig.7.과 같이 ID 거래 시스템, 암호키 관리 시스템, ID 거래 원장, ID 공유 원장, ID 보관 시스템, 분산 ID 거래 부정 탐지 시스템, 개발자, 운영자 등은 물리적 또는 논리적으로 네트워크를 분리하고, 접근통제시스템(ex-방화벽, 네트워크 접근통제, 서버접근통제, DB 접근통제 등)을 통해 비인가 접근을 차단한다.

② 악성코드 통제 : 보관자는 악성코드 감염에 의해 중요 자산(분산 ID, 암호키, ID 공유 원장, ID 거래 원장 등)의 위·변조 및 유출을 방지하기 위해 보호 대책을 수립, 이행하여야 한다.

③ 데이터 암호화 : 보관자는 ID 보관 시스템에 분산 ID를 보관시, 안전한 알고리즘으로 암호화해야 한다. 또한 보관자가 외부망과 통신하는 구간에는 전송 구간 암호화(ex-TLS)를 적용해야 한다.

④ 데이터 무결성 : 보관자는 보관하고 있는 분산 ID와 분산 ID 거래시 발생하는 모든 이벤트 내역을 기록하고 위·변조를 방지해야 한다. 이를 위해 보관자는 허가형(permissioned) 분산원장 네트워크 기반의 노드를 운영하면서 ID 거래 내역을 분산원장에 기록하여 관리하여야 한다.

⑤ 암호키 생성 및 이용 : 보관자는 분산 ID를 발급, 제출, 보관, 연계하는 과정에서 분산 ID를 암·복호화 하기 위한 암호키를 관리하고 그 이력을 기록 및 보관해야 한다. Fig.8.에서 보는 바와 같이 보관자는 암호키 관리 시스템(CKMS)으로부터 정보주체별 암호키를 생성하여 ID 보관 시스템에서 개인별로 분산 ID를 암·복호화하고, 보관자를 제외한 다른 객체들과는 정보 교환시 PKI 기반 비대칭 암호키로 서명하고 검증한다. 여기서 암호키 관리 시스템의 보

안성은 연결된 HSM(Hardware Security Module)의 보안성능과 직결되므로 NIST FIPS 140-2에서 정한 Level 4 등급[25]의 전용 장비를 권고한다.

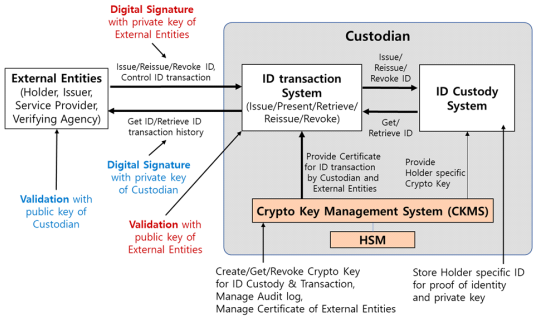

Fig. 8. Security Requirement for Crypto Key Management [24]

⑥ 로그 기록 및 보존 : 보관자는 분산 ID 거래 내역을 기록하고 일정기간 동안 보존해야 한다. Fig.9.와 같이 보관자는 허가형 분산원장 기반의 ID 거래 원장의 노드를 운영하고, 발급기관, 검증대행자, 통제자도 노드 운영에 참여하여 신뢰성을 보장한다. 원장 데이터는 타임스탬프, 거래 주체, 거래 유형, 실패 여부 등을 포함할 수 있다. 로그 기록에서 가장 중요한 것은 타임스탬프로, 모든 시스템의 시간 동기화가 전제 조건이 되어야 한다. 기록되는 모든 타임스탬프는 ID 거래 원장의 블록이 생성되는 해시 과정에 들어가는 타임스탬프를 기준으로 검증이 된다[26].

⑦ 비정상 거래 탐지 시스템 운영 : 통제자는 분산 ID를 거래하는 모든 작업 내역을 대상으로 비정상 거래를 탐지 및 모니터링 할 수 있어야 한다. 시스템을 통한 실시간 감시와 주기적인 감사를 통하여 비정상 거래 및 부정사용을 방지하여야 한다.

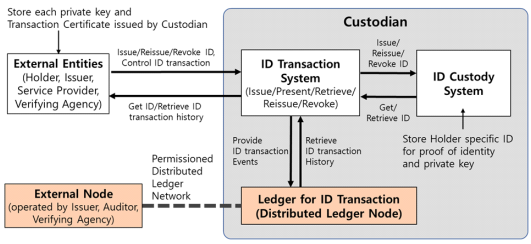

Fig. 9. Security Requirement for Log Recording and Maintenance [24]

4.4 기존 모델과의 비교분석

Table 1.을 보면, 본 장에서 제안한 분산 ID 보관 및 연계 서비스 모델을 적용하면 제3장에서 제기한 기존 모델의 문제점들에 대해 효과적으로 대응할 수 있다. 3.1 정보주체(이용자)의 보호 미흡에 해당하는 CT1과 CT2, 3.2 정보주체(이용자) 편리성 미흡에 해당하는 CT3, CT4가 보관자에 의한 분산 ID의 안전한 보관을 통해 해결될 수 있다. 또한, 3.3 상호 연동성 문제에 해당하는 CT5는 제안 모델을 확장한 ID 연계를 통해 해결될 수 있다.

발급기관으로부터 발급받은 분산 ID를 정보주체의 모바일 기기에 두지 않고, 보안 요구사항이 충족된 보관자의 시스템에 두게 되면, 모바일 기기에 대한 해킹이나 분실로 인한 정보 유출을 차단할 수 있다. 또한 보관자에 의한 안전한 보관 서비스 모델은 정보주체가 모바일 기기가 아닌 어떤 단말기를 사용하더라도 안전하게 ID 거래를 할 수 있다. 그리고 모바일 기기를 분실하거나 분산 ID를 모두 폐지 또는 재발급 받아야 하는 상황이 생기더라도 보관자를 통해 안전하게 본인 인증 절차만 거친다면, 정보주체의 불편함은 크게 줄어들게 된다. 무엇보다도 여러 도메인에서 개별적으로 분산 ID 서비스 모델이 생기더라도 분산원장 기반의 보관 및 연계 서비스 모델이 구축된다면 정보주체는 보다 다양한 서비스를 안전하게 받을 수 있게 된다.

또한, 제안 모델이 4.3.2절에서 기술한 보안 요구사항을 충족하게 되면 4.3.1절에서 식별된 보안 위협에 적절히 대응할 수 있다. Table 2.는 제안 모델의 보안 위협에 대하여 제시된 보안 요구사항이 통제 가능하다는 것을 나타낸다.

Table 1. Constraints solved by Proposed Model

Proposed Model	Constraints of Previous Model				
	CT1	CT2	CT3	CT4	CT5
Custody Model	○	○	○	○	
Federated Model					○

주[1] CT1 : Data leakage from hacking
CT2 : Data leakage from loss
CT3 : Limited terminal (mobile)
CT4 : Revocation and Reissue since loss
CT5 : Interoperability

Table 2. Security Requirements for Security Threats in the Proposed Model

Security Requirements	Security Threats					
	ST1	ST2	ST3	ST4	ST5	ST6
Network Separation	○	○		○		○
Malware Control	○		○		○	
Data Encryption	○	○		○		
Data Integrity			○			
Crypto key Control	○	○		○	○	
Log Recording			○			
Fraud Detection	○	○				○

주[1] ST1 : ID leakage by external attack
ST2 : Unauthorized use of ID by insiders
ST3 : ID transaction history tampering
ST4 : Crypto key leakage
ST5 : Application tampering
ST6 : Unauthorized access

제안 모델의 보관자 시스템에 접근 통제 시스템을 통한 네트워크 분리가 되면 외부 공격 및 내부자에 의한 ID 유출을 막고, 암호키 유출 및 비인가 접속을 차단할 수 있다. 악성코드 통제를 통해 ID 유출 및 거래내역, 어플리케이션의 위·변조를 차단할 수 있다. 데이터 암호화는 외부 공격 및 내부자에 의한 ID 유출과 암호키 유출을 방지할 수 있다. 데이터 무결성은 ID 거래 내역 위·변조를 방지하고, 암호키 생성 및 이용을 통해 ID 거래시 모든 정보를 안전하게 암·복호화하여 외부 공격 및 내부자에 의한 ID 유출과 암호키 유출을 차단하고 어플리케이션 위·변조를 방지할 수 있다. 로그 기록 및 보존을 통해서는 ID 거래 내역을 안전하게 보관하고, 비정상 거래 탐지 시스템을 통해서는 외부 공격에 의한 ID 유출과 내부자에 의한 ID 무단 도용을 막고, 비인가 접근에 대해서도 효과적으로 통제가 가능하다.

추가적으로 2.3절에서 설명한 기존 분산 ID 서비스 모델의 구조를 자세히 살펴보면, 현재 많이 사용하고 있는 PKI 기반의 인증 체계와 유사하다는 것을 알 수 있다. Fig.10.에 있는 사용자의 신원 정보를 안전하게 보관하는 전자지갑(e-wallet)은 공인인증서를 보관하는 NPKI 폴더와 유사하며, 블록체인

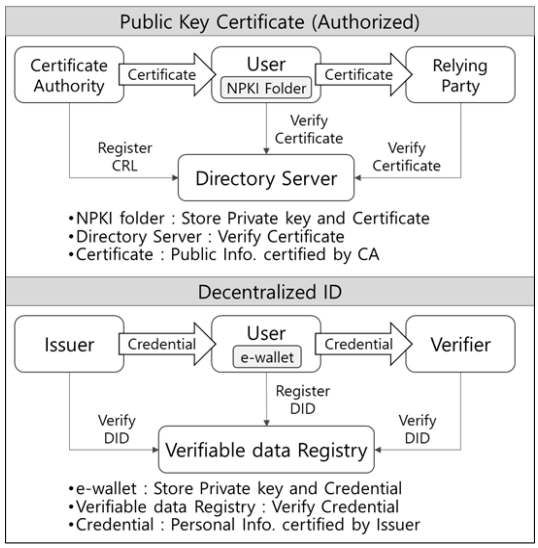

Fig. 10. Comparison of PKI Certificate with Decentralized ID System [4]

은 사용자의 공개키 등을 게시한다는 점에서 공인인증서의 디렉토리 서버 역할과 동일한 개념이다.

이렇게 분산 ID 서비스 기본 모델과 PKI 기반의 인증모델이 흡사하기 때문에 PKI 기반의 공인 인증 체계도 본 논문에서 제안하는 모델로 대체 또는 전환이 가능하다. 다만, 공인 인증 체계의 경우, 발급기관 역할을 하는 CA(Certificate Authority)를 관리하는 RootCA가 존재를 하고, 또 공인인증서를 발급하기 위해서는 CA가 아닌 RA(Register Authority)를 통해 정보를 등록하고 발급 대행을 하도록 하고 있어, 사용자들이 인증서를 발급하고 갱신하는 번거로움은 그대로 존재할 수밖에 없다. 우리나라에서는 사회적인 분위기상 공인인증서가 점차 사라지고 있는 상황에서 분산 ID를 이용한 인증 기술이 대체 수단으로 주목을 받고 있어 가능하면 안전하게 분산 ID를 보관 및 연계하는 서비스 모델로 전환되어야 할 것이다.

V. 결론 및 향후 발전 방향

분산원장기술을 이용한 분산 ID 서비스 모델은 해외에서도 많은 연구와 적용 사례가 나오고 있고, 국내에서도 유망한 사업 분야로 인식되면서 비즈니스를 선점하기 위해 여러 기업들간 경쟁이 심화되고 있다. 다만 아직까지는 공통된 기술 표준이 완전히 나오지 않다 보니, 여러 기업 또는 연합체에서 국제 또

는 국내 표준화 작업을 기다리지 못하고 조금씩 다르게 기술을 발전시켜 나가고 있는 실정이다. 이렇게 국가별로, 연합체별로, 도메인별로 조금씩 다른 기술, 다른 서비스 모델로 구현된다면 향후 상호 호환성 문제가 분명히 발목을 잡게 될 것이다. 마치 분산원장기술을 활용한 다양한 플랫폼이 등장한 이래로 여러 산업분야 또는 기업에 우후죽순으로 적용이 되었지만, 결국은 여기저기서 개별적으로 돌아가고 있는 현실이 그대로 반복될 수도 있다. 만약 그렇게 된다면, 정보주체는 자기 신원 정보의 주권은 찾을 수 있겠지만, 이기종 모델로 인해 서비스 사용에 불편을 겪게 될 것이다. 또한, 현재와 같이 정보주체가 활용할 수 있는 단말이 모바일 기기로 한정되어 있으면 모바일 기기 보안에 취약한 정보주체는 해킹으로 인한 정보 유출이나 분실(도난)으로 인한 신원 정보 관리의 어려움을 겪게 될 것이다.

이런 문제점들을 해결하기 위해 본 논문에서 별도의 안전한 보관자와 통제자를 추가하여 보다 개선된 분산 ID 보관 및 연계 서비스를 제안하였다. 정보주체가 데이터에 대한 자기 주권을 보장받으면서 보다 안전하고 편리하게 분산 ID를 사용할 수 있는 환경을 만들기 위해서는, 보관자 시스템에 대한 보안 강화와 통제자를 통한 모니터링 및 감사가 강화되어야 한다. 그런 면에서 향후 비정상 거래 탐지에 대한 케이스와 탐지 정책 개발이 보다 구체적으로 필요할 것이다. 또한, 제안 모델을 확장하여 여러 도메인간 연계 가능한 서비스를 만들기 위해서 분산 ID 기술을 개발하는 연합체나 기업들간 기술 표준과 그것을 적용하기 위한 공통 프로토콜에 대한 연구도 필요하다.

더 나아가서는 분산 ID의 정보주체를 사람으로만 국한시키지 않고, 다양한 주변 정보를 수집하는 사물인터넷(IoT)에도 적용할 수 있을 것이다. 수많은 IoT 디바이스(센서)를 통해 수집된 정보들은 데이터 처리를 위해 여과 없이 중앙서버로 모이게 되어 있다. 이 때, 분산 ID 개념을 IoT 보안에 접목시켜 각 디바이스별로 분산 ID를 발급받고, 수집되는 정보에 대해 주권을 행사하여 IoT 디바이스 관리부터 데이터 프라이버시 보호에도 적용하는 연구로 확장되기를 기대해 본다.

References

[1] S.R. Cho, D.S. Choi, S.H. Jin and H.H. Lee, "Passwordless authentication technology-FIDO," Electronics and Telecommunications Trends, 29(4), pp. 101-109, Aug. 2014

[2] Erika McCallister and Richard Brackney, "Information technology - security techniques - Entity authentication assurance framework" ISO/IEC DIS 29115, Dec. 2011

[3] Life With Alacrity, "The path to self-sovereign identity" http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverein-identity.html, Feb. 2020

[4] Hee-won Shim, "Domestic and overseas trends and implications of decentralized ID technology," Korea Financial Telecommunications & Clearings Institute, 73, Dec. 2019

[5] W3C, "W3C homepage" https://www.w3c.org, Mar. 2020

[6] DIF, "DIF hompage" https://identity.foundation, Mar. 2020

[7] Sovrin, "Sovrin homepage" https://sovrin.org, Mar. 2020

[8] P. Leach, M. Mealling and R. Salz, "A universally unique identifier (UUID) URN namespace," RFC 4122, July 2005

[9] Decentralized identifiers (DIDs) v1.0, "W3C Decentralized identifiers" https://www.w3.org/TR/2019/WD-did-core-20191127/, Mar. 2020

[10] Security Technology Research Team, "The concept and overseas technology trend of decentralized ID," e-Finance and Financial Security, 16, pp. 15-39, April 2019

[11] D.S. Kwon, H. Lee and J.D. Park, "Digital identity trend for digital trust society," Electronics and Telecommunications Trends, 34(3), pp. 114-124, June 2019

[12] Verifiable credentials data model 1.0, "Verifiable credentials" https://www.w

3.org/TR/2019/REC-vc-data-model-20191119/, Mar. 2020
〔13〕 SSImeetup Identity Webinar, "Trust frameworks and SSI: An interview with CULedger on the credit union MyCUID trust framework," https://ssimeetup.org/blog/page/5/, Feb. 2020
〔14〕 Steve Fulling, Phil Windley, Jason Law and Nathan George, "Indy, HIP identifier," Hyperledger Improvement Project(HIP), Mar. 2017
〔15〕 KISA Press release, "Collaboration for DID ecosystem between KISA and financial security institute," https://www.kisa.or.kr/notice/press_List.jsp, Feb. 2020
〔16〕 SK telecom Press release, "KOREA DID initial DAY," https://www.sktelecom.com/advertise/press_detail.do?idx=5122, Feb. 2020
〔17〕 DID Alliance, "DID Alliance" http://www.didalliance.or.kr/, Mar. 2020
〔18〕 MyID Alliance, "MyID Alliance" https:// myidalliance.org/, Mar. 2020
〔19〕 Connneting Lab, Blockchain Trend 2020, Business Books, pp. 85-94, June 2019
〔20〕 RaonSecure Press release , "Raonsecure MMA Blockchain" https://www.raoncorp.com/ko/about/news_list/view/28, Jan. 2020
〔21〕 DPASS, "Decentralized Passport" https://www.dpass.io/, Feb. 2020
〔22〕 LG CNS Blog IT Solutions/Security, " Security threats of smart phone," https://blog.lgcns.com/1106, Feb. 2020
〔23〕 Keundug Park, DaeKyung Kim and Heung Youl Youm, "Security enhancement for distributed ledger technology system based on open source," Korea Institute of Information Security and Cryptology, 29(4), Aug. 2019
〔24〕 Keundug Park and Heung Youl Youm, "Security requirements for digital asset transaction service model based on distributed ledger technology," TTAK. KO-12.0352, Dec. 2019
〔25〕 Information Technology Laboratory National Institute of Standards and Technology, "Security requirements for cryptographic modules," FIPS PUB 140-2, May 2001
〔26〕 Bitcoin.org, "Bitcoin : A peer-to-peer electronic cash system" https://bitcoin.org/bitcoin.pdf, Mar. 2020

〈저자소개〉

여 기 호 (Kiho Yeo) 종신회원
1999년 2월: 서강대학교 컴퓨터공학과 학사
2012년 8월: 건국대학교 정보통신대학원 정보보안전공 석사
2016년 2월: 순천향대학교 대학원 정보보호학과 박사과정 수료
2013년 3월~현재: 현대오토에버 블록체인서비스개발팀 책임연구원
〈관심분야〉 분산원장기술 보안, 자동차 보안, IoT 보안, 클라우드 보안, 정보보호관리체계

박 근 덕 (Keundug Park) 종신회원
1992년 2월: 동아대학교 전산공학과 학사
2015년 8월: 순천향대학교 대학원 정보보호학과 석사
2018년 2월: 순천향대학교 대학원 정보보호학과 박사
2018년 9월~현재: 서울외국어대학원대학교 국제교양학과 교수
2018년 3월~현재: 서울외국어대학원대학교 AI블록체인연구소 소장
2018년 9월~현재: TTA PG502 특별위원, PG1006 간사/특별위원
2018년 6월~현재: ISO/IEC JTC 1/SC 27 전문위원
2017년 8월~현재: ISO/TC 307 전문위원
2017년 2월~현재: ITU-T SG17 위원
2012년 2월~현재: 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증 심사원
〈관심분야〉 분산원장기술 보안, 정보보호관리체계, 개인정보보호, 클라우드 보안, 5G보안

염 흥 열 (Heung Youl Youm) 종신회원
1981년 2월: 한양대학교 전자공학과 학사
1983년 9월: 한양대학교 대학원 전자공학과 석사
1990년 2월: 한양대학교 대학원 전자공학과 박사
1982년 12월~1990년 9월: 한국전자통신연구원 선임연구원
1990년 9월~현재: 순천향대학교 공과대학 정보보호학과 정교수
2011년 1월~12월: 한국정보보호학회 회장(역), 명예회장(현재)
2007년 3월~현재: 한국인터넷진흥원 ISMS/PIMS 인증위원회 위원장
2009년~2016년: ITU-T SG17 부의장, ITU-T SG17 WP2/WP3 의장
2017년~현재: ITU-T SG17 의장
2016년 5월~현재: 개인정보보호표준포럼 의장
〈관심분야〉 정보보호관리체계, 개인정보보호, IoT 보안, 개인정보영향평가, 암호 프로토콜, 5G 보안, 분산원장기술 보안