디지털 신뢰 사회 실현을 위한 디지털 아이덴티티 동향

Digital Identity Trend for Digital Trust Society

권동승 (D.S. Kwon, dskwon@etri.re.kr) 초연결기술기획실 책임연구원/실장
이현 (H. Lee, hyunlee@etri.re.kr) 초연결기술기획실 책임연구원
박종대 (J.D. Park, parkjd@etri.re.kr) 블록체인기술연구센터 책임연구원/센터장

ABSTRACT

The Internet was designed for machines, not humans, and hence, nobody owns a digital identity. Instead, a digital identity is rented from a website and an application. This lack of unique and secure digital identities has resulted in confusion in the online/cyber world. Digital identities pose one of the oldest and most difficult problems with regard to the Internet. There is still no way to use digital credentials to prove, own, and control an online identity, namely a self-sovereign identity, in the same manner we do in the offline world, particularly without a trusted third party. This article discusses the current open standards for digital identities, proposes solutions pertaining to digital identities in the future, and introduces the concept of a blockchain-based self-sovereign digital identity without the need of trusted third parties.

KEYWORDS Digital Identity, Self Sovereign Identity

Ⅰ. 서론

사람들은 인터넷으로 정보의 공유·전달을 넘어 더 현실적인 가치를 점차 관리·교환하기 시작하였다. 즉, 웹 사용이 증가함에 따라 수억 명의 사람이 온라인으로 비즈니스 및 경제 행위 등을 하기 위해 해당 사이트의 화면에 나타나는 거의 모든 입력 양식에 이름, 비밀번호 및 개인 식별 정보를 무심하게 입력하고 있다. 그러나 방문자가 방문하는 사이트의 진위를 평가할 수 있는 일관되고 이해하기 쉬운 프레임 워크가 없으며, 개인정보가 불법적인 당사자에게 공개되어도 이를 확인하는 신뢰할

* DOI: 10.22648/ETRI.2019.J.340312
* 이 논문은 2019년도 정부의 지원을 받아 ETRI 에서 수행된 연구임[19ZH1200, 데이터 안심사회를 위한 트러스트 데이터 커넥톰 원천기술 개발].

수 있는 방법을 알 수 없다.

인터넷은 태생적으로 신뢰할 수 있는 상대방과 신뢰할 수 있는 환경에서 동작하게 만들어진 인터넷의 한계로 인터넷으로 디지털화된 전 세계의 모든 것이 연결되는 초연결 지능정보사회에서 근본적으로 신뢰의 한계에 직면하고 있다. 인터넷은 태생적으로 누가 당신에게 연결되어 있는지 알 수 있는 방법 없이 구축되어 있어서 우리가 인터넷을 신뢰할 수 있는 방안을 마련하지 않으면, 인터넷에 대한 대중의 신뢰를 누적적으로 침해할 수 있는 도난 및 기만이 급증하는 상황에 직면할 것이다.

현 인터넷 아이덴티티는 전문 공격자의 공격을 견딜 수 없다. 이런 위기가 심화되면 인터넷 기반의 경제 거래에 대한 신뢰와 수용을 잃기 시작할 것이다. 인터넷 공격자는 개별 소비자 자신이 상대방을 알 수 있는 능력이 없다는 점을 이용하여 '피싱(Phishing)'을 통해 은행 및 기타 정보를 탈취하거나 컴퓨터에 있는 '스파이웨어'를 실수로 설치하게 하여 장기간 '파밍(Pharming)' 공격하여 정보를 수집하도록 유도한다. 또한, 방대한 아이덴티티를 보유한 기업, 정부 등의 데이터베이스를 타깃으로 삼아 수십만 개의 신원을 한 번에 훔치기도 한다. 피싱 및 파밍은 현재 컴퓨터 업계에서 가장 빠르게 성장하는 인터넷의 신뢰를 저하시키는 기술 중 하나로 연간 복합 성장률(CAGR: Compound Annual Growth Rate)이 1,000%이다. 2005년 2월의 피싱 동향 그룹 '피싱 동향 보고서'에는 피싱 사이트에서 7월에서 다음 해 2월 사이에 월 26%의 연평균 성장률을 나타내며, 복합 연평균 1,600%의 성장률을 보인 것으로 조사되었다.

이러한 피해를 막기 위하여 표준화된 디지털 신원 서비스를 인터넷에 추가하는 것이 시도되고 있다. 공개 도메인에 대한 연결을 보호하기 위해 Secure Socket Layer(SSL)를 사용하는 것과 같이 특정 도메인에서 부분적으로 성공했으며, 기업 내 Kerberos 그리고 최근에는 Business-to-Business(B2B) 아이덴티티 공유에서 성공적인 연합 사례가 있으나, 이 성공은 아이덴티티 패치 워크를 인터넷을 통해 합리적인 구조로 변형시키는 데는 거의 기여하지 못했다. 따라서 이 아이덴티티 계층 없이 현재의 인터넷 서비스는 아이덴티티 정보 일회용 패치 워크를 기반으로 하므로 미래의 사이버 물리 공간까지 초연결 지능정보 사회에서 웹 서비스의 이점을 얻지 못할 것이다. 따라서 미래에는 인터넷에서 신뢰 상실을 방지하고 인터넷 사용자에게 사이버 공간과 관련된 안전성, 개인정보 및 확실성에 대한 깊은 이해를 어떻게 전달할 수 있는가가 더욱 더 중요해진다.

디지털 아이덴티티에는 중앙집중형 아이덴티티, 제 삼자 아이덴티티 제공자 기반의 아이덴티티, 분산원장 혹은 블록체인기반의 자기 주권 아이덴티티 세 가지 모델로 구분할 수 있다.

첫째, 중앙집중형 아이덴티티는 사용자가 외부 사이트에 이름과 비밀번호로 계정을 만들고 두 당사자가 기밀성과 데이터 무결성이 보장된 상태로 서로 식별 및 인증하여 통신할 수 있는 암호화 프로토콜로서 Transport Layer Security(TLS) 프로토콜과 SSL 프로토콜이 있다. 두 프로토콜의 기본적인 주요 목표는 기밀성(때로는 사생활 보호), 데이터 무결성, 아이덴티티 및 디지털 인증서를 사용한 인증을 제공하는 것이다.

둘째, 아이덴티티 제공자 기반의 아이덴티티는 두 당사자 중간에 아이덴티티의 신뢰를 보장하는 아이덴티티 제공자가 있는 것으로 Security Assertion Markup Language(SAML), OAuth, Open ID connect 등의 표준이 있다.

셋째, 최근에 연구·개발 중인 자기 주권을 보장하는 블록체인기반 아이덴티티는 두 당사자의

신뢰를 블록체인기반으로 인증하는 것이다. 관련된 공개 표준으로는 World Wide Web Consortium(W3C)의 검증할 수 있는 자격 증명(Verifiable Credentials)과 Decentralized Identifiers(DIDs)가 있고, OASIS의 탈중앙화된 키 관리 시스템, Internet Engineering Task Force(IETF), Digital Identity Foundation(DIF)의 DID Auth, 그리고 SOVRIN 재단[1]의 제 삼의 인증기관이 필요 없는 영구적인 아이덴티티가 있다.

본 논문에서는 아이덴티티에 관련 공개 표준기술 현황을 간략히 소개하고, 현 디지털 아이덴티티 관련 이슈를 분석·정리하였고, 마지막으로 최근에 연구되고 있는 블록체인기반의 자기 주권 아이덴티티 연구 현황을 소개하고자 한다.

Ⅱ. 아이덴티티 공개 표준기술 현황

우리는 아날로그를 디지털로 전환(Digitization)하였고, 프로세스를 디지털화(Digitalization)하였으며, 이제 효과 창출을 위한 디지털 트랜스포메이션 시대에 진입하고 있다. 이 디지털 트랜스포메이션 시대에는 개인별로 3~4개의 모바일 디바이스와 응용에 대응하는 복수의 아이덴티티, 다양한 SNS별로 다수의 아이덴티티, 그리고 클라우드 기반의 응용과 서비스를 이용하기 위한 다수의 아이덴티티, 초연결로 내가 소유하고 있는 Internet of Things(IoT)별 아이덴티티를 보유하고 있지만, 아이덴티티가 공통 계층이 아니고 부적절하게 관리되는 사이버 공격면의 확대는 전문화된 사이버 공격자는 쉽게 아이덴티티를 탈취할 수 있게 되었다. 따라서 마이크로소프트는 사람, 사물과 프로세스를 안전하게 연결하기 위해서 전체적이고 통합적인 아이덴티티에 대한 공개 표준을 제안하였다[2]. 이 공개 표준은 고용인, 동업자, 고객, 유통업자, 공급자, 디바이스와 사물 간 연결을 위해 공통의 아이덴티티 플랫폼, 도난당한 디바이스의 불법적인 연결을 지능적으로 차단할 수 있는 아이덴티티 플랫폼, 산업체의 요구사항을 수용하고 데이터 프라이버시를 보장하는 신뢰하는 아이덴티티 플랫폼 그리고 계속 진화하는 사이버 공격을 실시간 검출·자기 경감·자동화 치료를 할 수 있는 내재화된 기계학습 기능을 보유한 내재화된 정보보호를 포함하여야 한다. 이 전체적인 아이덴티티 솔루션은 OAUTH, Open ID connect, Fast IDentity Online(FIDO), SAML, System for Cross-domain Identity Management(SCIM), Oracle Database Attacking Tool(ODAT), JSON, DIF, Token Binding, Open Identity Exchange 등이 통합되도록 설계되어야 한다.

유연하지 않고 폐쇄적이며 도메인에 국한된 오래된 독점 인증 프로토콜로는 IBM사의 Network Basic Input/Output System(NetBIOS)과 LU 6.2, 마이크로소프트사의 NT LAN Manager(NTLM), Basic Auth(HTTP에서 기본적인 액세스 인증)와 Passport(사용자 인증을 위한 온라인 인증 시스템), 노벨사의 Internetwork Packet eXchange(IPX) 등이 있다.

처음으로 광범위하게 채택된 아이덴티티 표준인 Lightweight Directory Access Protocol(LDAP)은 TCP/IP 위에서 디렉터리 서비스를 조회하고 수정하는 응용 프로토콜이다. SAML은 인증 정보 제공자와 서비스 제공자 간의 인증 및 인가 데이터를 교환하기 위한 XML 기반의 개방형 표준 데이터 포맷으로 처음으로 광범위하게 채택된 연방 프로토콜(Federation Protocol)로서 가장 중요한 요구사항은 웹 브라우저 통합인증이다.

OAuth는 인터넷 사용자들이 비밀번호를 제공하지 않고 다른 웹사이트상의 자신들의 정보에 대해 웹사이트나 애플리케이션의 접근 권한을 부여할

수 있는 공통적인 수단으로써 사용되는, 접근 위임을 위한 개방형 표준으로 기존 인증 방법인 아이디와 비밀번호의 보안상 취약점을 보완한 것이다. OAuth 1.0은 사용자와 디바이스를 차별화시키고, 클라우드 API를 보호하는 데 최적화되어 있다. OAuth 2.0과 Open ID Connect는 개발자의 채택 장벽을 낮추고, 모바일, 기업과 클라우드를 위해 설계된 첫 번째 통합된 인증과 허가 모델로서 확장성이 내재되어 있다.

그럼에도 2017년 버라이즌 커뮤니케이션스가 작성한 데이터 위반 보고서에 의하면 데이터 위반의 81%가 보안이 취약하거나 도난당한 비밀번호를 포함한 것으로 조사되었다. 따라서 더 편리하면서 안전한 방법을 찾게 되었다.

따라서 비밀번호 사용의 한계 극복을 위해 인증 프로토콜과 인증 수단을 분리하여 비밀번호 없이 인증 강도를 높이면서 사용자의 편리성을 높여 스마트 모바일 환경에 적합한 인증 기술인 FIDO가 제시되었다[3]. FIDO 1.0은 2-factor 인증을 위해 표준 기반 하드웨어를 사용하였고, FIDO 2.0은 표준 기반 하드웨어 없는 인증이다. 비밀번호 없는 인증이 더 안전한 이유는 중앙화된 생체정보 저장소 없이 사설 암호 키를 사용하는 것으로 사용자가 가지고 있는 생체정보와 사용자의 현재 상황이라는 두 가지 요소를 사용한다는 점이다.

따라서 현재는 사용자 경험과 정보보호를 향상시키게 되었으나, 공격자들은 웹 응용을 위한 다양한 보안 토큰(HTTP 쿠키, OAuth 토큰)은 종종 분실되거나 도난당할 수 있으므로 중간자 공격이나 재생 공격에 취약한 문제점이 있다. 이를 해소하기 위한 IETF 규격인 토큰 바인딩은 TLS 연결의 양 끝에 암호화 인증서를 사용하여 TLS 보안을 향상시키는 목적으로 TLS를 확장시킨 방법이다. 이 토큰 바인딩 프로토콜은 클라이언트-서버 응용이 다중 TLS 세션과 연결로 확장된 오래 지속되고 고유하게 식별 가능한 TLS 바인딩을 생성할 수 있게 한다. 그런 다음 응용 프로그램은 보안 토큰을 TLS 계층에 암호학적으로 바인딩하여 토큰 내보내기 및 재생 공격을 방지한다. 프라이버시 보호를 위해 토큰 바인딩 식별자는 TLS를 통해서만 전달되며, 언제든지 사용자가 재설정될 수 있다.

글자와 숫자로 된 비밀번호는 인간이 기억하기에는 어렵지만, 컴퓨터가 추측하기는 쉽고 모바일 디바이스에 비밀번호를 입력하는 것은 불편하며 복수의 서비스에 재사용한다는 것은 공격 면적을 증가시키며, 심지어 강력한 비밀번호도 쉽게 피싱될 수 있는 문제가 있다. 최근의 FIDO는 더 안전하지만, 기존 방식 대비 더 복잡하고 사용하기에 약간 불편한 점이 있다. 따라서 매우 안전하면서도 사용하기에 매우 편리한 아이덴티티가 필요하다.

이 비밀번호의 대안으로 제 삼의 신뢰하는 인증기관을 이용한 비대칭 키를 사용한 접속 방법이 있다. 사용자가 응용 서버에 키로 접속하면 응용 서버는 인증기관에 해당 키의 사용 여부를 문의하고, 사용자는 생체정보, PIN, 접촉 등의 제스처를 이용하여 해당 키 사용을 허가하면 인증기관은 응용 서버에 해당 키 사용을 서명하며, 응용 서버는 서명을 검증하고 사용자 접속을 허용하는 것이다. 인증기관은 인증을 위한 사설 키를 안전하게 사용하게 하며 사용자의 제스처에 의해서만 동작한다. 따라서 인증기관은 이전의 비밀번호 같은 어떤 비밀정보를 가지고 있지 않으며, 대신에 사용자의 제스처에 의해서만 허용되는 쌍의 사설 키만을 가지고 서명한다. 이를 기반으로 한 표준은 W3C의 Web Authentication(WebAuthn)과 Client to Authenticator Protocol(FIDO2 CTAP)가 있다. 따라서 공통 사용 가능한 비밀번호 없는 인증에 대한 새로운 표준으로 사용자의 제스처를 표현하는 방법으로 스마트

디바이스가 주목받고 있다.

이 디바이스를 이용한 방법으로 Global System for Mobile Communications Association(GSMA)은 스마트폰으로 편리함을 희생시키지 않으면서 다중 인증하는 것을 가능하게 하는 Mobile Connect를 만들었다[4]. 이 기술은 모바일 전화번호를 사용자 식별번호로, 모바일 폰을 인증자로, 모바일 네트워크 사업자는 인증과 아이덴티티 제공자로 역할을 분담하여 비밀번호와 하드웨어 보안 토큰을 대체하는 것이다[5]. 이 Mobile Connect 인증은 공개 표준인 OpenID Connect를 이용하여 분산되고 연합된 프레임워크이다. OpenID Connect는 비영리재단인 OpenID 재단에서 관리하는 인증 수단으로서 분산형 디지털 아이덴티티 시스템이다. 이 프레임워크는 온라인 서비스 제공자에게 인증, 허가, 사용자 아이덴티티 검증 등 아이덴티티 서비스를 제공하고 있다. 이 프레임워크에서 연합된 사용자 인증은 연합된 아이덴티티 프레임워크로, 연합된 아이덴티티 프레임워크는 탈중앙화된 아이덴티티로 진화하고 있다.

III. 아이덴티티 현안 이슈

IBM에서는 디지털 트랜스포메이션으로 야기될 수 있는 사이버 범죄와 아이덴티티 위조에 대응하기 위한 디지털 트러스트 프레임워크로 보증, 인증, 통찰과 통합의 네 가지 요소를 통하여 끊김 없는 종단 사용자 경험을 지원하고, 상황 맞춤의 트러스트 레벨과 더 강화된 보안을 제공하면서 비즈니스 요구에 기반한 새로운 정책을 쉽게 구현하고자 한다[5]. IBM에서는 아이덴티티의 디지털 트러스트를 확립하기 위해 위조 방지를 만족시켜 응용 혹은 서비스로부터 관심을 제거하는 보안 상호작용을 최소화할 수 있고, 종단 간 디지털 생활을 통해 사용자에 대해 점진적으로 배우며, 상호작용 레벨을 증가시켰다.

마이크로소프트의 Kim Cameron은 인터넷에 아이덴티티 계층의 성공과 실패를 좌우하는 일곱 가지를 제시하였다[6].

첫 번째는 사용자 제어 및 동의이다. 어떤 상황에서도 사용자의 동의하에 아이덴티티가 공개되고, 필요시 요청 당사자의 신원 확인도 할 수 있다. 또한, 인터넷에서 사용자 정보의 흐름을 추적하고 필요시 제어할 수 있어야 한다.

두 번째는 아이덴티티를 제한된 사용에 대한 최소한의 공개이다. 즉, 가장 적은 양의 아이덴티티 정보 제공과 아이덴티티 사용을 제한할 수 있어야 한다. 그리고 아이덴티티의 불법적 사용이 항상 가능하다는 것을 바탕으로 아이덴티티 시스템을 구축해야 한다. 즉, 최소한의 아이덴티티 정보 공개 원칙을 바탕으로 구축된 시스템은 신원 도용에 덜 매력적이며 위험을 더욱 줄일 수 있다.

세 번째는 정당한 당사자이다. 아이덴티티 확인 시스템은 식별 정보의 공개가 주어진 아이덴티티 관계에서 필요하고 정당한 당사자로 제한되도록 설계되어야 한다. 이 시스템은 사용자가 정보를 공유하는 동안 상호작용하는 당사자를 인식할 수 있도록 해야 한다.

네 번째는 지시된 신원이다. 범용의 아이덴티티 확인 시스템은 공공 기관에서 사용하는 '무지향성' 식별자와 사설 기관에서 사용할 수 있는 '단방향' 식별자 모두를 지원해야 하므로 불필요한 상관관계 해제를 방지하면서 접근이 쉬워야 한다.

다섯 번째는 운영자와 기술의 다원주의이다. 범용 아이덴티티 시스템은 각자가 동시에, 그리고 다른 맥락에서 시민, 직원, 고객 및 가상의 인물이라는 것을 인정하면서도 차별화를 받아들일 수 있도록 여러 신원 제공 업체가 운영하는 다중 신

원 기술의 상호 작동을 전달하고 활성화될 수 있어야 한다.

여섯 번째는 인간 통합이다. 아이덴티티 시스템이 인간 사용자로 확장되고 통합되어야 한다. 범용 아이덴티티 시스템은 인간 사용자를 식별 공격에 대해 보호 기능을 제공하는 인간-기계 통신 메커니즘을 통해 통합된 분산 시스템의 구성 요소로 정의한다.

일곱 번째는 컨텍스트 간 일관된 경험이다. 통합 아이덴티티 시스템은 여러 운영자와 기술을 통해 상황 분리가 가능하면서 사용자에게 간단하고 일관된 경험을 보장해야 한다.

인터넷에서 아이덴티티 계층을 만드는 것의 어려움은 기업, 금융 산업, 정부, SNS, 포털 서비스 사업자, 정보보호 관계자 등 다양한 이해당사자가 필요로 하는 공통 사항을 기본 프레임 워크에 포함시키는 것에 동의하지 않기 때문이다. 예를 들어 기업은 고객 및 직원과의 관계를 핵심 자산으로 보고 있으며, 이들을 치열하게 보호하기 때문에 그들이 자신의 선택을 제한하거나 디지털 관계를 어떻게 만들고 표현하는지에 대한 통제력 포기를 기대하는 것은 어렵다. 금융 산업과 같은 특정 업종별 클러스터는 고객과 디지털 관계를 유지하고자 하는 고유한 의도를 가지고 있다. 마지막으로 멀웨어 및 아이덴티티 도용은 모든 인터넷 사용자에게 중요한 관심사인 프라이버시 문제를 야기한다. 그렇기 때문에 특정 구현의 내부 복잡성으로부터 응용을 보호하고 디지털 아이덴티티를 느슨하게 결합하지만, 누가 인터넷에 연결되어 있는지 확증시켜 줄 수 있는 확실한 통합 아이덴티티 시스템이 필요하다.

현재 인터넷을 이용한 소셜네트워크 활동, 교육, 시민권, 온라인 게임, 취미활동, 직장, 기업이 제공하는 서비스, 인터넷 거래 등을 위해서 응용과 서비스별로 사용자 이름과 비밀번호라는 아이덴티티를 사용하고 있다. 즉 아이덴티티로 인터넷상의 모든 활동을 하는 모든 것이므로, 당신의 아이덴티티 수는 응용 숫자보다 많다. 따라서 아이덴티티의 불법적 사용, 개인 데이터의 끊임없는 불법적 사용, 감시를 위한 비용 증가 등 우리의 아이덴티티가 위험에 노출되어 있다[7]. 이를 해소하기 위해 개인, 기업, 정부는 아이덴티티에 대해 다음 사항을 요청하고 있다. 즉, 사용자가 통제할 수 있는 아이덴티티를 필요로 한다.

- 개인은 아이덴티티와 데이터에 대한 통제와 프라이버시, 해커로부터 보호, 불법 사용으로부터 보호
- 기업은 신뢰하지만 진실, 모두와 협력, General Data Protection Regulation(GDPR), 구매자 신원확인(KYC: Know Your Customer)/자금 세탁방지(AML: Ante-Money Laundering)를 위한 위험 감소
- 정부는 국경과 대리인을 위한 아이덴티티, 난민을 위한 디지털 아이덴티티, 모든 사람의 사회 및 금융 활동을 위한 아이덴티티

그리고 2018년 5월 25일 시행된 유럽의 개인정보보호법인 GDPR은 정보 주체의 권리와 기업의 책임성 강화, 개인정보의 유럽연합 역외 이전 요건 명확화 등을 주요 내용으로 한다. 이 내용 중 정보 주체의 권리로 개인이 생산한 데이터 권리의 보장과 이 데이터 처리로 야기되는 문제까지 해소하기 위해 데이터 생산자(사람, 조직, 사물)의 위조 불가능한 아이덴티티가 필요하다. 즉, 4차 산업혁명의 원유로 인정되는 데이터의 소유권을 보장하는 수단으로 새로운 아이덴티티가 필요하다. 더불어 디지털 사이버 세상에서 잊힐 권리를 아이덴티티로 실현할 수 있는가에 대한 연구도 필요하다.

IV. 블록체인기반 아이덴티티 기술 동향

많은 사람이 매일 경험하듯이 전 세계는 디지털 및 물리적 현실이 하나로 통합되어 생활 방식이 흐려지는 글로벌 디지털 트랜스포메이션을 겪고 있다. 이 새로운 물리 및 디지털 세계에서도 개인의 사생활과 보안을 향상시키기 위해 디지털 신원에 대한 새로운 모델이 필요하다. 이를 위해 무수한 앱 및 서비스에 대한 광범위한 동의를 제공하고 수많은 제공 업체에 아이덴티티 데이터를 분산시키기보다는 개인이 신원 데이터를 저장하고 액세스를 쉽게 제어할 수 있는 안전한 암호화된 디지털 허브에 대한 연구가 진행되고 있다. 즉, 우리 모두는 디지털 아이덴티티의 모든 요소를 안전하게 그리고 개인적으로 저장·소유·제어할 수 있는 디지털 아이덴티티가 필요하다. 이 아이덴티티는 사용하기 쉬워야 하며, 개인의 아이덴티티 데이터가 어떻게 액세스되고 사용되는지에 대한 완전한 제어를 할 수 있어야 한다.

이를 실현하기 위한 DIF은 개방적인 DIDs 생태계를 구축하고, 모든 참가자 간의 상호작용을 보장하기 위해 필요한 기본 요소를 개발하는 데 중점을 둔 엔지니어링기반 조직이다[8]. 이 산하에는 식별자, 이름 및 검색 작업반, 저장 및 계산 작업반, 그리고 클레임 및 자격증명 작업반이 있다.

- 식별자, 이름 및 검색 작업반은 식별자의 중앙집중형 시스템 없이 사람, 조직 및 장치를 식별하고 찾을 수 있는 방법으로 블록체인 및 분산원장에서 분산 식별자 및 이름의 생성, 확인 및 검색을 가능하게 하는 프로토콜 및 구현 중이다.
- 저장 및 계산 작업반은 안전하고 암호화된 프라이버시 보호 저장 및 데이터 계산을 한다. 식별자와 이름은 소유 주체에 대해 자체 주권을 가져야 하므로 사용자의 ID 데이터는 사적으로 유지되어야 하며, 허용된 엔티티에서만 액세스하는 기능을 제공하도록 공급자에 무관하게 어디서든지 동작되는 솔루션에 대한 사양 및 참조 구현 중이다.
- 클레임 및 자격증명 작업반은 소유권 주장 및 주장을 검증할 수 있는 기술을 생태계 참가자 및 고객이 DID로 서명된 클레임을 자신의 앱과 서비스에 쉽게 통합할 수 있도록 생태계에 제공할 수 있는 사양, 프로토콜 및 도구를 정의하는 작업을 최근에 시작하였다.

마이크로소프트사는 2017년부터 개인 프라이버시, 보안과 제어를 향상시키기 위해 처음부터 다시 시작하여 설계된 DIDs를 만들기 위해 블록체인 혹은 다른 분산원장기술을 사용하는 것에 투자하였고, 지난 2월에 ID2020에 가입하였다. ID2020은 공식적으로 인정된 아이덴티티 없이 살고 있는 전 세계 1.1억 명에게 정치적, 경제적 그리고 사회적 기회를 제공하기 위한 재단이다[9]. 마이크로소프트가 DIDs를 만들면서 배운 것은 다음과 같다[10].

- 아이덴티티의 소유와 제어를 위해 분산형 스토리지 시스템, 컨센서스 프로토콜, 블록체인 및 다양한 신흥 표준을 검토한 결과, 블록체인 기술 및 프로토콜이 DID를 구현하는 데 적합
- 프라이버시가 처음부터 내장
- 신뢰는 커뮤니티에 의해 세워지고 개인에 의해 축적됨. 분산시스템에서 신뢰는 다른 단체가 보증하는 증명에 기반하여 자신의 정체성을 증명
- 사용자 중심의 앱과 서비스: DID 및 ID 허브를 사용하면 개발자가 사용자를 대신하여

정보를 제어하는 대신 이 정보를 처리하여 법률 및 규정 준수 위험을 줄일 수 있음
- 개방적인 상호운용: 모든 사람이 액세스할 수 있는 강력한 분산 ID 환경을 구축하려면 표준 오픈 소스 기술, 프로토콜 및 참조 구현을 토대로 구축
- 세계적인 규모의 확장성: 광대한 규모의 사용자, 조직 및 장치를 지원하려면 기본 기술이 기존 시스템과 동등한 수준으로 확장 및 성능을 수행할 수 있어야 함
- 모두에게 접근 가능성을 제공

가트너는 2017년 12월 Blockchain: Evolving Decentralized Identity Design 보고서에서 인간이 물리적인 생활을 출생증명서로 시작하는 것과 동일하게 사람들은 사이버상의 디지털 생활을 자기 주권 아이덴티티로 시작한다고 하였다[11]. 이 디지털 아이덴티티 실현을 위한 Digital Identity Foundation(DIF), SOVRIN 재단[1]과 Evernym[12]의 연구개발 현황을 정리하였다.

디지털 아이덴티티는 인터넷에서 가장 오래되고 가장 어려운 문제 중 하나이다. 오프라인 세상과 동일한 방법으로 온라인 아이덴티티를 증명하는 디지털 증명서는 사용할 방법이 아직은 없었지만, 이제 막 연구개발이 진행되고 있다. W3C에서는 디지털 서명된 증명서포맷을 표준화하고 있고, 공개 블록체인은 디지털 서명을 검증하기 위해 필요한 공개 키의 탈중앙화된 등록과 발견을 제공한다. SOVRIN은 이 두 가지를 기반으로 어떤 중앙기관에 의존하지 않으며 절대 뺏어갈 수 없으며, 평생 휴대용 디지털 아이덴티티인 자기 주권 아이덴티티를 위해 글로벌 공개 유틸리티를 만드는 방법을 제시한다. 거버넌스(SOVRIN재단과 SOVRIN 신뢰 프레임워크), 확장성(검사와 관찰 노드 그리고 증명), 액세스 능력(최소한의 비용과 최대 가용성)이 포함한 SOVRIN 네트워크는 이 목적을 달성하기 위해 독점적으로 설계했다. 가장 중요한 것은 쌍의 익명 식별자, 점대점 사설 에이전트, 영지식 증명의 암호를 사용한 개인 데이터의 선별적 공개를 포함하여 글로벌 스케일로 프라이버스를 설계의 기본으로 하였다. 증명 발행자, 소유자 그리고 검증자를 위한 경제적 인센티브를 제공하기 위해 SOVRIN 프로토콜은 프라이버시가 보호되는 가치 교환을 표방하게 설계된 디지털 토큰을 포함하였다.

그림 1은 자기 주권 아이덴티티 개념을 나타낸 것이다[13]. 우선 글로벌로 공유하고 프라이버시가 보호되는 DIDs를 가지고 있는 블록체인상의 분산원장, 탈중앙화된 키 관리시스템(DKMs: Decentralized Key Management System)을 가지고 있는 디지털 지갑, 그리고 상대방으로 구성된다. W3C의 DIDs 신택스는 RFC 8141 URN(Uniform Resource Name, 통합자원 이름) 기반의 scheme:method:method-specific identifier로 구성되며, 자기 서술을 위한 DID, 검증을 위한 공개 키, 인증을 위한 Auth 프로토콜, 상호작용을 위한 서비스 종착

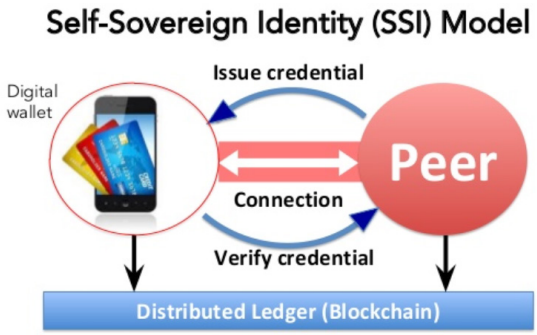

그림 1 자기 주권 아이덴티티 개념

출처 D. Reed, R. Cranston, and J. Esser, "Trust Frameworks and SSI: An Interview with CULedger on the Credit Union MyCUID Trust Framework," SlideShare, July, 2018. CC BY-SA 4.0.

점, 감사를 위한 타임 스탬프, 무결성을 위한 서명의 표준 요소가 있다. DKMs는 DIDs에서 필요한 사설 키를 관리하기 위한 제안된 공개 표준이다. DID Auth는 DID 소유자가 사설 키의 제어를 증명에 의해 인증하는 간단한 표준방법이다. Verifiable Credentials는 디지털 세계에서 물리 세계의 증명서와 동일한 역할을 하는 것으로 사진, 이름, 식별번호 등 증명할 주제와 관련된 정보, 발행 기관과 관련된 정보, 증명이 어떻게 도출되었는가에 대한 증거, 그리고 만료일 정보를 포함한다.

개인의 아이덴티티를 소유하고 제어할 수 있는 DIDs는 다음의 절차로 생성되고 활용된다.

(1) 사용자는 블록체인상에 DID 생성을 요청한다.
(2) 블록체인은 사용자의 DID를 회신한다. DID는 분산 식별자의 상태를 설명하기 위한 공통 문서 형식을 정의하는 W3C 사양을 준수한다.
(3) 사용자는 DID 기반으로 사설 키를 생성한다.
(4) 디지털 지갑에 있는 DKMs에 저장된 이 키를 기반으로 DID Auth로 본인 인증을 하고, 외부와 정보 요청·전달·거래 등을 수행한다.

SOVRIN의 검증 가능한 자격증명 과정이 W3C와 다른 점은 그림 2와 같이 발행자와 소유자 간 그리고 소유자와 검증자 간에 쌍으로 된 유일한 DIDs를 사용하고 영지식 증명(Zero-knowledge proof)을 사용한다는 점이다. SOVRIN은 DIDs를 목적으로 구축된 분산원장 플랫폼인 Hyperledger Indy 기반으로 아이덴티티의 글로벌 공개 유틸리티로 제공하기 위한 신뢰 프레임워크의 형태로 거버넌스, 비즈니스, 그리고 법적인 규칙을 추가하였다.

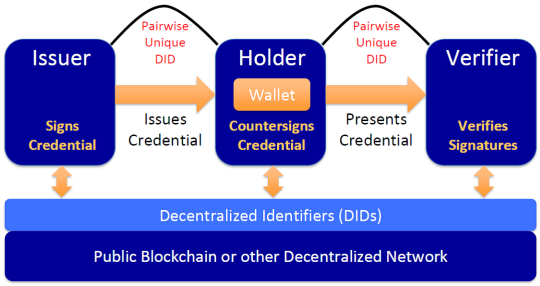

그림 2 SOVRIN의 검증 가능한 자격증명 동작

출처 D. Reed, R. Cranston, and J. Esser, "Trust Frameworks and SSI: An Interview with CULedger on the Credit Union MyCUID Trust Framework," SlideShare, July, 2018. CC BY-SA 4.0.

Evernym사는 자기 주권 아이덴티티를 어떤 중간자도 염탐할 수 없으며 제거할 수 없는 영원성·유일성·휴대성·안전성·검증가능성 등의 요구사항을 추구하고 있다. 따라서 DID를 만드는 것만으로는 신뢰할 수 없으므로, 신뢰하기 위해서는 상대방에 증명할 수 있어야 한다. 즉 수신자는 누가 자격증명을 발행했는지, 단지 프레젠터에게만 발행되었는지, 변경되지 않았는지, 그리고 발행자가 철회하지 않았는지를 중간자 없이 검사할 수 있어야 한다. 중간자와 연결 브로커 없는 상황에서도 블록체인기반의 DIDs와 검증할 수 있는 자격증명을 조합하면 연결성, 보안과 신뢰를 실현할 수 있다. SOVRIN 재단과 긴밀한 기술적 협력을 하는 Evernym사는 Verifiable claims를 위한 자기 주권 아이덴티티에 대한 솔루션을 다음 세 가지 사항을 고려하였다.

- 트러스트: 중앙화된 데이터베이스 없이도 개인, 지관, 사물 등에 의해 만들어진 클레임의 진위를 즉시 정확하게 검증
- 프라이버시: 현존하는 가장 강력한 프라이버시 보호 기술
- 상호호환성: 레거시와 원장기반의 아이덴티티 모두와 범용적인 호환성을 제공

또한, Evernym사는 SOVRIN의 자기 주권 아이덴티티를 위한 글로벌 공개 유틸리티라는 아이덴티티 프레임워크 기반으로 탈중앙화된 아이덴티티 인프라 플랫폼(아이덴티티 소유자 툴, 클레임 제기 및 트러스트 앵커 서비스, 클레임 교환과 검증 툴, 탈중앙화된 응용 스택)을 제공한다.

V. 결론

인터넷은 사람이 아니라 기계를 연결하기 위해 설계되었고, 현재 어느 누구도 디지털 아이덴티티를 가지고 있지 않으며, 대신에 웹사이트나 응용으로부터 아이덴티티를 빌려서 사용하고 있다. 이로 인해 비효율적이고, 불법적이며, 프라이버스가 침해받는 혼란을 야기했고, 사용자와 상호작용하는 업체, 기관은 사용자 개인정보를 대용량 데이터베이스에 저장함으로써 해커의 대상이 되었고, 누구나 데이터를 저장해야 하는 악의적인 책임을 만들었다. 즉, 디지털 아이덴티티는 인터넷에서 가장 오래되고 가장 어려운 문제 중 하나이다. 그리고 4차 산업혁명 시대의 디지털 원유인 데이터의 소유와 제어, 즉 주권을 확보할 수 있는 수단으로서 자기 주권 아이덴티티가 연구되고 있다.

자기 주권 아이덴티티는 오프라인 세상과 달리 아이덴티티를 증명해 줄 믿을만한 외부 기관이 없는 상황에서 온라인 세상의 안전하고 유일한 아이덴티티 증명과 더불어 데이터에 대한 개인의 소유와 제어를 실현하고자 한다. 이 실현을 위해 DIF, W3C, SOVRIN, Evernym 등이 연구개발을 진행 중이지만, 아직은 초기 단계이므로 우리도 현존하는 인터넷 구조에 기반한 신뢰할 수 있는 초연결 지능정보사회를 실현하기 위한 방안으로 자기 주권 아이덴티티에 대한 연구가 필요하다.

용어해설

AML(Ante-Money Laundering) 국내외적으로 이루어지는 불법 자금의 세탁을 적발 및 예방하기 위한 법적·제도적 장치로서 사법제도, 금융제도, 국제협력을 연계하는 종합 관리시스템

GDPR(General Data Protection Regulation) 2018년 5월 25일 시행된 유럽의 개인정보보호 법령으로 정보 주체의 권리와 기업의 책임성 강화, 개인정보의 유럽연합 외 이전 요건 명확화 등을 주요 내용으로 함

KYC(Know Your Customer) 금융거래 사고를 방지하기 위해 구매자의 신분을 확인하고 검증하는 절차

W3C(World Wide Web Consortium) 국제 웹 표준화 기구의 하나. WWW의 표준안 제작과 새로운 표준안 제안, 기술의 공유를 통해 WWW의 기술적·사회적 확산을 위해 구성된 전 세계적 단체로 1994년 10월에 설립됨

약어 정리

AML	Ante-Money Laundering
B2B	Business-to-Business
CAGR	Compound Annual Growth Rate
CTAP	Client to Authenticator Protocol
DIDs	Decentralized Identifiers
DID Auth	DID-based Authentication
DIF	Digital Identity Foundation
DKMs	Decentralized Key Management Systems
FIDO	Fast Identity Online
GDPR	General Data Protection Regulation
GSMA	Global System for Mobile Communications Association
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
ID	Identity
IoT	Internet of Things
IPX	Internetwork packet Exchange
JSON	JavaScript Object Notation
KYC	Know Your Customer
LDAP	Lightweight Directory Access Protocol
NetBIOS	Network Basic Input/Output System

OAuth	Open Authorization
ODAT	Oracle Database Attacking Tool
PIN	Personal Identification Number
SAML	Security Assertion Markup Language
SCIM	System for Cross-domain Identity Management
SNS	Social Networking Service
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
URN	Uniform Resource Name
W3C	World Wide Web Consortium
WebAuthn	Web Authentication
XML	eXtensible Markup Language

참고문헌

[1] SOVRIN, available at https://sovrin.org/

[2] J. Chik, "Planning for Tomorrow - Connecting Identities for People, Process, and Things," Microsoft, eic2018.

[3] 조상래 외, "패스워드 없는 인증기술-FIDO," 전자통신동향분석, 제29권 제4호, 2014. 8, pp. 101-109.

[4] GSMA, "Mobile Connect," GSMA, 2018. available at https://www.gsma.com/identity/mobile-connect

[5] S. Vax, "Fighting cybercrime and identity fraud in the digital age," IBM, 2018.

[6] C. Kim, "The Laws of Identity," May 2005, available at http://www.identityblog.com/?p=352

[7] A. Simons, "Decentralized Identity for a Decentralized World," Microsoft, eic2018.

[8] DIF, available at https://identity.foundation/

[9] ID2020, available at https://id2020.org/

[10] A. Simons, "Decentralized digital identities and blockchain: The future as we see it," Microsoft, Feb. 2018. Available at https://www.microsoft.com/en-us/microsoft-365/blog/2018/02/12/decentralized-digital-identities-and-blockchain-the-future-as-we-see-it/

[11] H. Farahmand, "Blockchain: Evolving Decentralized Identity Design," Dec. 2017. Available at https://www.gartner.com/doc/3834863

[12] evernym, available at https://www.evernym.com/

[13] N. George, "Self-Sovereign Identity 101-An introduction to Multi-sourced Identity and the core open standard for Self-Sovereign Identity," sovrin foundation, eic2018.