탈중앙화 신원증명 기술 동향

김수형 개인정보보호/ID관리/블록체인 보안(PG502) 의장, 한국전자통신연구원 기술총괄

1. 머리말

모든 것이 '0'과 '1'로 표현되는 디지털 세계에서도 현실과 마찬가지로 사람들은 만나고 소통하며, 자신의 자격을 증명하고 정당한 서비스를 받거나 자신이 직접 생산한 콘텐츠를 배포하기도 한다. 디지털화가 점차 가속화되면서 사람들이 현실보다 디지털 세계에 더 많은 시간을 소비하며, 경제·사회·문화 활동을 경험할 날도 멀지 않았다. 현실과 가상이 융합된 메타버스[1] 세상이 도래하면 현실에 실체를 둔 명품 시계나 가방보다 디지털 이미지로 표현된 명품이 좀 더 효율적인 자기표현 수단이 될지도 모른다.

마찬가지로 현실에서 사용되는 플라스틱 카드 형태의 신분증보다 디지털화되어 네트워크를 통해 전달될 수 있는 디지털(모바일) 신분증이 더 많이 활용될 것은 누구나 예상해 볼 수 있다. 사용자가 접하는 대부분 서비스의 시작 지점에서 사용자의 신원을 확인하기 위한 수단은 필요하기에, 사용자의 다양한 자격을 증명하는 디지털 신분증의 등장과 점진적 확산은 필연적이다. 본고에서 다루는 탈중앙화 신원증명 기술은 이러한 디지털 신분증의 확산을 가속화 하는 기반 기술로 활용이 예상된다. 또한, 디지털 세상의 가장 중요한 자산인 데이터가 일부 플랫폼에 집중화되어 독점되는 문제를 해결하기 위한 방향으로 제시된 '탈중앙화 웹(web3.0)'과 마찬가지로, 사용자의 신원증명 정보가 특정 기관에 저장·관리되고 해당 기관을 통해 제공하는 중앙집중형 ID 관리(centralized identity management) 모델의 문제와 한계를 극복하고자 사용자 스스로 신원증명 정보를 관리하고 선택적으로 제공하는 탈중앙화 신원 관리(decentralized identity management) 모델이 제시되었고 관련 기술은 계속 진화하고 있다[2].

본고에서는 이러한 탈중앙화 신원증명 기술의 간략한 배경을 소개하고 현재 신원증명 서비스 간 상호 연동을 위해 개발되는 기술들을 최근 제정된 혹은 제정될 표준에 기반하여 설명하고자 한다.

2. 기술 등장 배경 및 주요 표준

2.1 등장 배경

현재 인터넷 서비스에서 익숙하게 활용되는 사용자 인증 기술은 대부분 중앙집중형 ID 관리 모델에 기반한다. 사용자의 신원(identity) 정보를 신뢰할 수 있는 인증기관에 저장하고 해당 인증기관이 서비스 기관에 필요한 신원을 제공하거나 보증해 주는 방식의 중앙집중형 ID 관리 모델은 SAML[3], OAuth[4] 등 산업계에서 오랜 기간 검증된 표준 기술에 기반해 신원증명을

위한 핵심 솔루션으로 활용되었다.
하지만 최근의 환경 변화로 중앙집중형 ID 관리 모델이 갖는 근본적 문제가 제기되면서 탈중앙화 신원증명 기술에 관심이 커지기 시작했다. 첫 번째 문제는 신원정보 유출 사고가 계속해서 발생하는 것이다. 중앙집중형 모델에서는 중앙서버에 모든 사용자의 신원정보를 관리하기 때문에 최고의 해킹방지 솔루션을 적용하더라도 근본적인 해결은 어렵다. 둘째로, 국내외적인 개인정보보호 강화 추세에 따라 데이터 '자기주권'이 데이터 경제 시대의 해결 과제가 되었기 때문이다. 사용자 스스로 신원정보를 통제하기 위한 수단이 요구되었고, 서비스 기관에서는 다른 서비스 기관에만 머물러 있는 고부가 사용자 데이터를 사용자 동의 하에 획득할 방안이 요구되었다. 세 번째는 개별 서비스마다 신원정보를 등록하고 관리해야 하는 불편함에 있다. 기술의 발전으로 서비스는 계속 새로워지지만, 사용자의 등록·인증 절차가 여전히 불편하다는 것은 해결되어야 할 문제이다.
이러한 문제들을 해결하기 위한 기술로 탈중앙화 신원증명 기술이 소개되었다. 이와 관련하여 2017년경 자기주권 신원(Self-Sovereign Identity)[5] 개념의 등장, W3C의 탈중앙화 식별자(DID, Decentralized Identifiers)와 검증 가능한 크리덴셜(VC, Verifiable Credential) 표준, 탈중앙화 신원증명 기술의 개발 및 상호 연동을 위한 산업체 연합인 DIF(Decentralized Identity Foundation), 관련 오픈소스 프로젝트 등이 주목받았다.

2.2 주요 표준

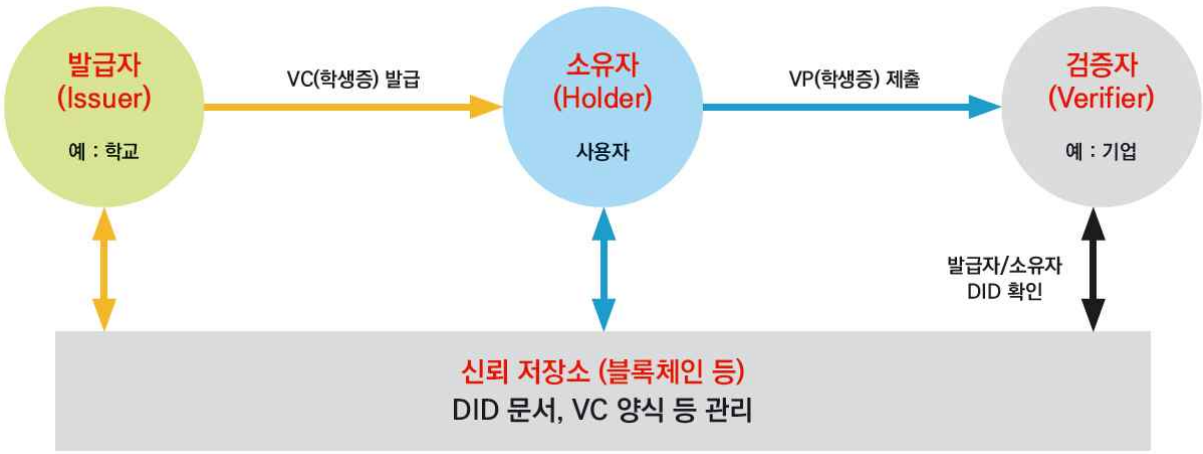
2.2.1 탈중앙화 식별자 (Decentralized Identifier)

탈중앙화 식별자(이하 DID)[6]는 웹 관련 표준을 개발하는 사설표준화기구 W3C의 Decentralized Identifier Working Group에 의해 2022년 7월 제정이 완료된 표준이다. 사용자(또는 기기, 서비스, 조직 등)에 대한 탈중앙화 디지털 신원을 구현하기 위한 아키텍처, 데이터 모델 등을 정의한다. DID는 중앙관리기구가 필요하지 않으며, DID의 식별 대상(즉, 사용자)의 통제 하에 관리된다. 모든 DID는 해당 식별 대상에 대한 기본적인 정보를 포함하는 DID 문서(Document)와 연결되며, DID 문서의 신뢰성 보장 및 접근 용이성을 위해 블록체인 등 신뢰할 수 있는 저장소에 저장 관리된다. DID 문서는 식별 대상이 서명한 문서를 암호학적으로 검증하거나 암호 통신 등을 수행하기 위한 공개키 정보와 식별 대상과 소통할 수 있는 서비스 엔드포인트(endpoint) 등의 정보로 구성된다.

2.2.2 검증 가능한 크리덴셜 (VC, Verifiable Credential)

검증 가능한 크리덴셜(이하 VC)[7]은 W3C의 Verifiable Credentials Working Group에 의해 2019년 11월 표준 제정(v1.0)을 완료하고 2022년 3월 개정(v1.1)되었다. VC는 운전면허증, 학위증명서, 여권 등 현실 세계의 신분증을 디지털 세계에서 활용할 수 있는 방법을 제공한다. VC는 암호학적으로 안전하고 프라이버시를 보존하며 기계가 검증할 수 있는 방식으로 디지털 세상에서 필요한 다양한 종류의 크리덴셜을 제공할 수 있다. 이를 위해 VC는 물리적인 형태의 신분증과 같이 사용자에 대한 다양한 신원 속성(attribute)을 포함할 수 있으며, 디지털 서명을 이용해 VC 정보의 무결성을 검증할 방안을 제공한다.

VC 기반의 탈중앙화 신원증명 서비스는 [그림 1]과 같은 발급자(issuer), 소유자(holder), 검증자(verifier) 및 신뢰 저장소(verifiable data registry)의 역할(role)을 갖는 개체(entity)들로 구성된다. 발급자는 소유자에게 VC를 발급하고 소유자는 발급된 VC를 디지털지갑을 통해 관리하고 서비스 이용에 필요한 VP(Verifiable Presentation, 소유자가 검증자에게 전달하기 위해 VC를 이용해 생성된 데이터)를 검증자에게 제출한다. 검증자는 제출된 VP를 검증하기 위해 신뢰 저장소로부터 검증에 필요한 정보(예: 발급자/소유자의 DID 문서)를 받아 확인하는 기본 절차를 갖는다. 참고로, 디지털지갑을 통해 사용자가 직접 신원정보를 관리하는 부담을 해결하고자, 기본 모델과는 다르게 제3자에 위탁 관리하는 모델 등에 대해서 국제표준화가 진행 중이다[8].

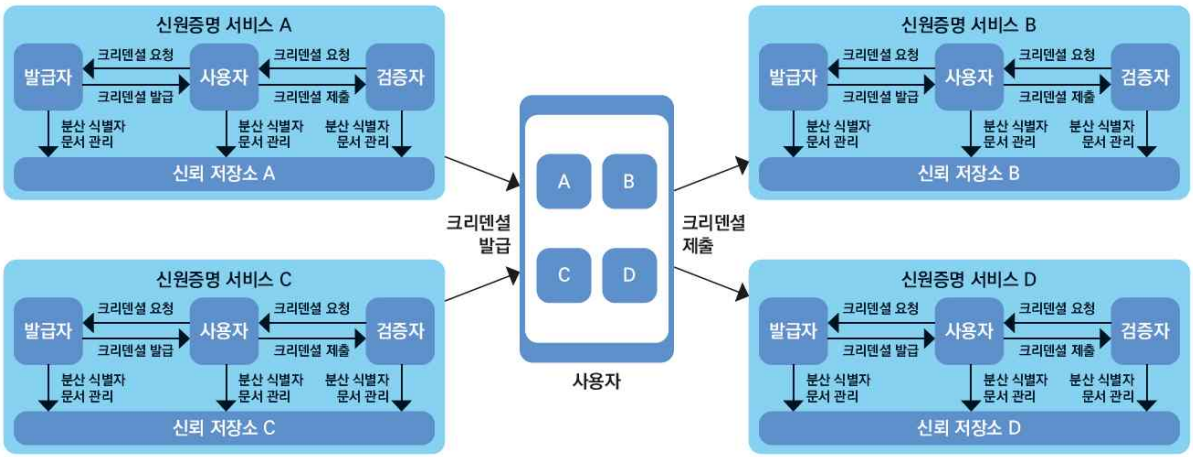


[그림 1] 탈중앙화 신원증명 기본 모델

3. 기술 동향

3.1 서비스 간 상호연동 문제

최근 다양한 응용 분야에서 탈중앙화 신원증명 서비스를 활용함에 따라 [그림 2]와 같이 사용자가 두 개 이상의 서비스를 이용하는 환경을 고려할 필요가 있다. 이에 2021년 12월에 제정된 국내표준[9]에서는 서로 다른 신원증명 서비스를 동시에 이용하는 경우에 발생 가능한 상호연동 문제들을 정의하고 있다. 첫째로 검증자가 소속되지 않는 신원증명 서비스에서 발급된 크리덴셜을 사용자가 전달할 경우, 검증자는 크리덴셜에 대한 무결성 검증뿐만 아니라 크리덴셜 발급자에 대한 신뢰 여부를 판단할 수 있어야 하는데 검증자가 사전에 모든 크리덴셜 발급자와 신뢰 관계를 설정하는 것은 불가능하여 크리덴셜 발급자의 신뢰 여부를 결정하는 데 어려움이 있다. 두 번째로 사용자 측면에서는 신원증명 서비스별 제공되는 디지털지갑을 사용자 기기마다 설치하고 동일 크리덴셜을 중복해서 발급받아야 하는 문제와 서비스가 요구하는 크리덴셜을 찾아서 제출하는 데 불편이 있다. 세 번째로 동일 신원정보를 포함하는 크리덴셜일지라도 서비스마다 다양한 양식(schema)으로 발급될 수 있어서 검증자가 전달받은 크리덴셜을 기계적으로 해석하기 어려울 수 있다는 것이다. 위와 같은 문제들은 탈중앙화 식별자의 상호연동을 위해 기존에 개발된 DID 리졸버(resolver)[10] 기술만으로는 해결이 어렵다.



※ 출처: TTA표준[9]

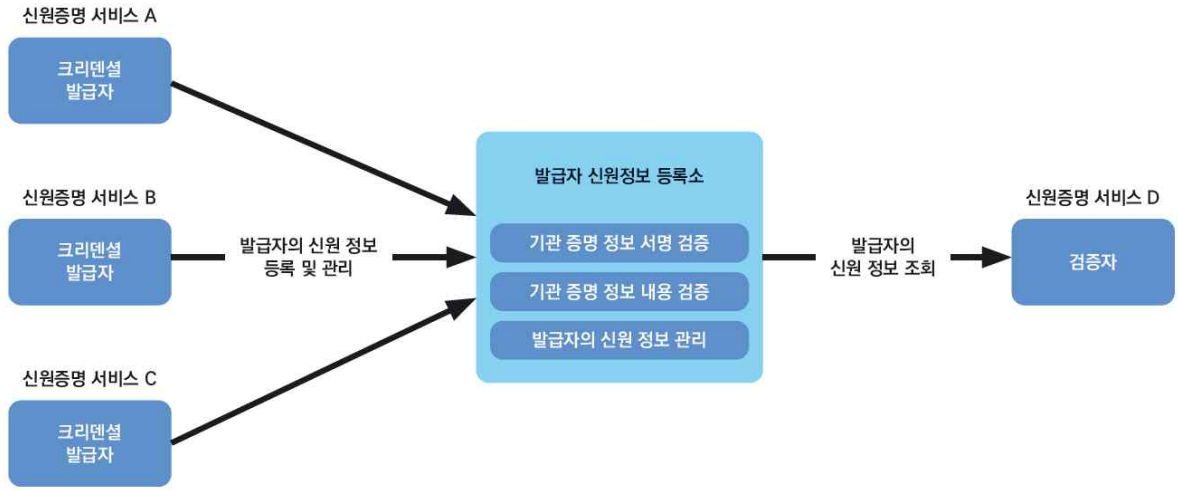
[그림 2] 사용자의 다중 신원증명 서비스 이용 환경

3.2 발급자 신원정보 관리

발급자와 검증자가 서로 다른 신원증명 서비스에 속해 있는 경우에 검증자는 사용자가 전달한 크리덴셜의 발급자에 대한 신뢰 여부를 결정할 수 있어야 한다. 크리덴셜의 신뢰도는 크리덴셜에 포함된 사용자 신원정보를 보증하는 발급자의 신뢰도에 따라 결정되기 때문이다. 예를 들어, 학생의 성적증명은 해당 학생이 졸업한 학교에서 발행한 증명서가 아닌 학생 본인 또는 타 기관의 증명서는 신뢰성에 문제가 있다. 따라서 입사희망자로부터 성적증명서(크리덴셜)를 받는 기업(검증자)은 해당 학교(발급자) DID 문서를 통해 성적증명서의 위변조를 검증하고, 동시에 크리덴셜 발급자의 DID가 실제 학생이 졸업한 학교의 DID인지 확인할 수 있어야 한다. 발급자(학교)와 검증자(기업)가 동일 신원증명 서비스에 속한 경우에는 해당 서비스 도메인의 신뢰 관리 체계에 의한 기술적 방법 또는 정책을 통해 확신할 수 있으나, 발급자와 검증자가 서로 다른 신원증명 서비스에 속한 경우에 발급자 DID가 실제 학교의 DID인지 판단할 근거를 제공하기 어렵다. 이에, 2021년 12월 제정된 국내표준[11]은 해당 근거를 제공하기 위한 기술적 방안을 제시한다. 해당 표준에서는 발급자의 신원을 보증하는 발급자 신원정보 등록소라는 새로운 참여자를 정의한다. 발급자 신원정보 등록소는 발급자가 어느 신원증명 서비스에 속해 있는지와 무관하게, 발급자의 신원을 증명하기 위한 정보(기관 DID 정보, 기관 기본 정보, 기관 증명 정보 등)를 관리하고, 검증자가 요청한 발급자의 신원정보를 제공하는 기능을 수행한다. 위에서 예를 들었던 기업은 성적증명서의 발급자가 학생이 졸업한 학교와 일치하는지를 발급자 신원정보 등록소로부터 조회하여 확인할 수 있다.

3.3 통합 크리덴셜 관리

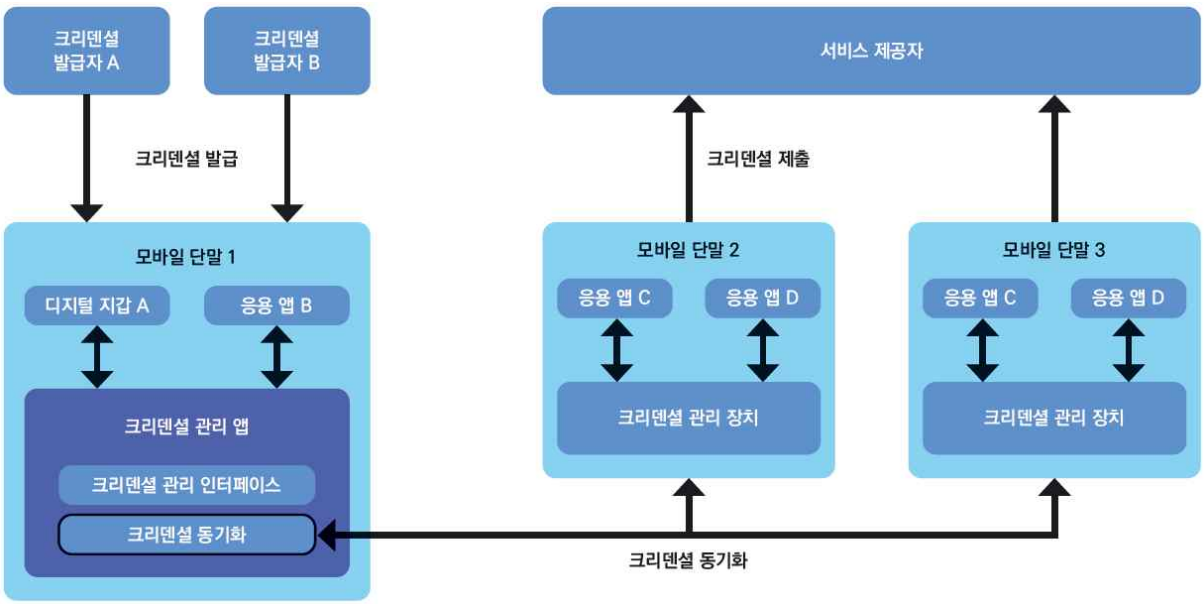
탈중앙화 신원증명 서비스에서는 사용자가 직접 크리덴셜을 관리할 수 있도록 디지털지갑 응용(앱)이 제공된다. 현재 서비스별로 디지털지갑이 제공되고 있어, 사용자는 자신이 소유한 단말마다 지갑을 설치하고 동일 크리덴셜을 중복해서 발급받는 불편이 있을 수 있다. 또한, 사용자가 지갑마다 어떠한 크리덴셜이 관리되는지 사전에 파악하기 어려우므로 서비스를 이용할 때 요청된 크리덴셜을 편리하게 조회하고 제출하기도 어렵다. 2021년 12월에 제정된 국내표준



※ 출처: TTA표준[11]

[그림 3] 발급자 신원정보 등록소 개념도

[12]에서는 위에 설명된 문제를 다루기 위한 요구사항과 기능을 정의한다. [그림 4]와 같이 사용자가 다수의 사용자 단말과 앱을 이용하는 환경에서 크리덴셜을 안전하게 통합 관리하고 필요시 편리하게 조회하여 사용할 수 있는 크리덴셜 관리 방안과 한번 발급한 크리덴셜을 사용자 단말마다 중복 발급 없이 사용할 수 있는 크리덴셜 동기화 기능을 정의한다. 해당 표준에 의하면 통합 크리덴셜 관리 앱을 통해 사용자 신원정보가 필요한 다양한 응용 앱에 응용이 속한 서비스 도메인과 상관없이 크리덴셜을 선택적으로 전달할 수 있다.



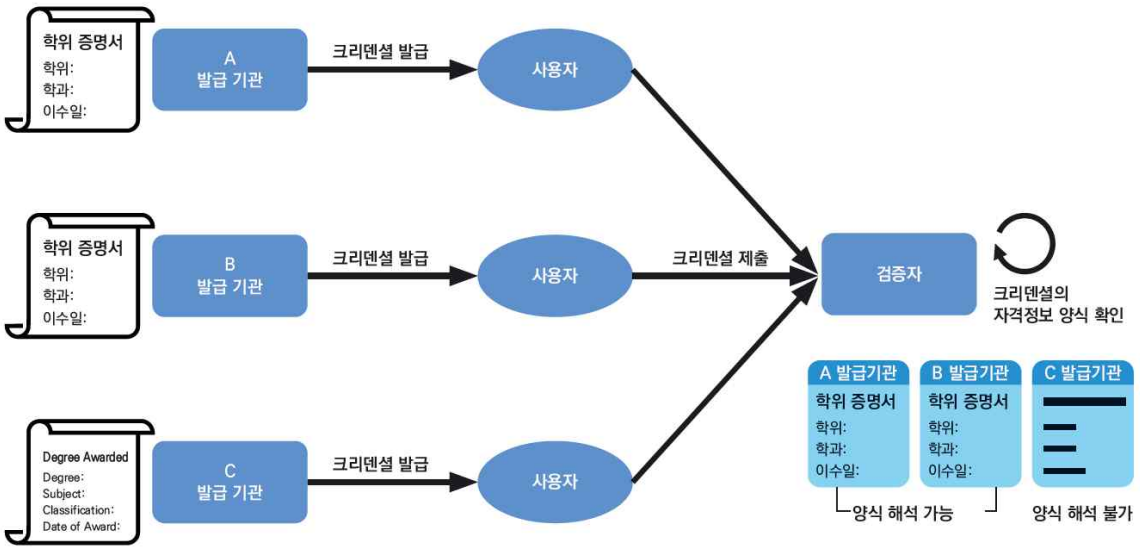
※ 출처: TTA표준[12]

[그림 4] 통합 크리덴셜 관리 구조

3.4 크리덴셜 양식 변환

동일 신원정보를 포함한 크리덴셜이라 하더라도 발급 기관마다 서로 다른 양식을 사용할 수

있으며, 국외에서 크리덴셜을 발급받을 수도 있다. 따라서 서비스 간 상호 연동을 위해 검증자가 다양한 유형의 양식으로 구성된 크리덴셜을 검증할 방안이 제공되어야 한다. 특별한 방안이 없다면 검증자는 크리덴셜을 해석하는데 상당한 수작업이 요구될 수 있다. 향후 크리덴셜 양식이 표준화 및 법/제도 등으로 통일되지 않는 이상 양식의 다양성은 피할 수 없으며, 이는 탈중앙화 신원증명 서비스의 확장성과 상호운용성을 저해하는 장애가 될 수 있다. 이에 TTA PG502에서는 2022년 12월 제정을 목표로 검증자가 해석할 수 없는 크리덴셜 양식을 해석 가능한 양식으로 자동변환하기 위한 요구사항 및 기능 정의에 대한 표준을 개발 중이다.



※ 출처: TTA PG502

[그림 5] 크리덴셜 양식 변환 필요성

3.5 크리덴셜 위임

현실 서비스 환경에서 대리 서명, 위임장 작성, 미성년자의 법정대리인 등 본인을 대신할 대리자를 지정하여 일시적으로 본인의 권한이나 신원정보를 위임하는 사례가 있다. 탈중앙화 신원증명 서비스를 통해 발행된 크리덴셜을 현실 서비스 환경에 맞춰 운영하기 위해서는 크리덴셜을 다른 사용자에게 위임하는 기능이 요구될 수 있다. 이에, 2021년 제정된 국내표준[13]은 탈중앙화 신원증명 서비스에서 크리덴셜 위임을 위한 요구사항 및 기능을 정의한다. 해당 표준에서는 위임자가 이미 자신이 가지고 있는 권한에 대한 정보를 대리자에게 위임하고자 하는 경우와 기존 발급받은 크리덴셜을 기반으로 위임 크리덴셜을 발급하는 경우의 두 가지 시나리오에 기반한 요구사항 및 기능을 정의한다.

4. 맺음말

본고는 탈중앙화 신원증명 서비스가 등장한 배경과 주요 표준 기술을 소개하고, 서비스 간 상호연동 문제를 해결하기 위해서 최근 개발된 기술들을 관련 표준을 중심으로 정리하였다. 상호연동 문제는 서비스 확장과 사용자 편의를 위해 반드시 해결해야 하는 과제이다. 소수의 기업에서만 인정받는 디지털 졸업증명서, 일부 공공서비스에만 적용된 모바일 신분증 등과 같이 사

용에 제약이 있는 신원증명 서비스는 탈중앙화 신원증명 기술이 지향하는 방향에 부합하지도 않지만, 사용자의 불편으로 인해 기술 확산에 큰 걸림돌이 될 것이다. 본고에서 설명된 상호연동 기술이 이러한 걸림돌을 모두 긍정적인 방향으로 해결할 기술인지는 좀 더 검토가 필요하나 충분한 참고가 되리라 기대된다.

최근 FIDO[14]는 '패스키(passkey)[15]'를 발표하며 패스워드 없는(passwordless authentication) 세상을 실현하기 위해서 상호경쟁 관계인 애플, 구글, 마이크로소프트가 협력해 FIDO의 편의성 향상을 위한 기술을 지원할 계획임을 밝혔다. 이러한 지원은 2015년부터 앱 환경에서 패스워드를 대체하기 시작한 FIDO 기술을 웹(브라우저) 환경에서도 조만간 일상적으로 경험하게 되리라는 기대를 낳았다. 탈중앙화 신원증명 기술도 마찬가지로 '디지털 신분증 시대'를 앞당길 핵심 솔루션으로 자리 잡기 위해서, 사용자에게 기술이 부담으로 받아들여지지 않도록, 사용자 편의성 개선 및 상호 연동을 위해 관련 생태계에 속한 기업/기관/연구자들의 협력이 필요한 시점이다.

※ 본 연구는 과학기술정보통신부의 재원으로 정보통신기획평가원의 지원을 받아 수행됨 [No.2020-0-00321, 5G 서비스 환경에서 프라이버시가 보장되는 자기통제형 분산 디지털 신원 관리 및 보안기술 개발]

[주요 용어 풀이]

- FIDO (Fast IDentity Online): 패스워드 방식보다 간편하고 보안성 높은 사용자 인증 서비스를 제공하기 위해 개발된 개방형 인증 표준 기술
- 크리덴셜 (Credential): 신원이나 자격을 증명하면서 증거로 제출된 데이터 집합(출처: ISO/IEC 29003)으로서 본고에서는 디지털 신분증, 신원증명서 등으로 설명됨

[참고문헌]

[1] 메타버스 기술 및 표준 동향과 R&D 추진방향, TTA 저널, 2022.03
[2] 경계없는 세상과 사용자 인증기술 동향, 전자통신동향분석, 2021.08
[3] OASIS SAML(Security Assertion Markup Language) v2.0 고찰 및 활용, 한국멀티미디어학회지, 2006.03
[4] https://oauth.net/2/, OAuth 2.0
[5] The Inevitable Rise of Self-Sovereign Identity, The Sovrin Foundation, 2017.03
[6] Decentralized Identifiers (DIDs) v1.0, W3C, 2022.07
[7] Verifiable Credentials Data Model v1.1, W3C, 2022.03
[8] 탈중앙화 신원관리 서비스 모델, TTA 저널, 2021.01
[9] 다중 분산 신원 관리 서비스를 위한 상호연동 프레임워크 - 제1부: 공통 요구사항, TTA 표준, 2021.12
[10] 분산ID를 활용한 신원관리 프레임워크 제2부: 신원증명 및 상호연동 방법, TTA 표준, 2020.12

[11] 다중 분산 신원 관리 서비스를 위한 상호연동 프레임워크 - 제2부: 발급자 신원정보 관리, TTA 표준, 2021.12
[12] 다중 분산 신원 관리 서비스를 위한 상호연동 프레임워크 - 제3부: 크리덴셜 관리, TTA 표준, 2021.12
[13] 분산ID 기반 서비스에서의 크리덴셜 위임을 위한 기능 요구사항, TTA 표준, 2021.12
[14] Special Report - FIDO 기술 표준화 동향, TTA 저널, 2017.07
[15] White Paper: Multi-Device FIDO Credentials(PassKey), FIDO Alliance, 2022.03

※ 출처: TTA 저널 제203호