경계없는 세상과 사용자 인증기술 동향

World Without Boundaries and Trends in User Authentication Technology

진승헌 (S.-H. Jin, jinsh@etri.re.kr) 신인증·물리보안연구실 책임연구원
조진만 (J.-M. Cho, zmzo@etri.re.kr) 신인증·물리보안연구실 책임연구원
조상래 (S.R. Cho, sangrae@etri.re.kr) 신인증·물리보안연구실 책임연구원
조영섭 (Y.S. Cho, yscho@etri.re.kr) 신인증·물리보안연구실 책임연구원
김수형 (S.H. Kim, lifewsky@etri.re.kr) 신인증·물리보안연구실 책임연구원/기술총괄

ABSTRACT

The field of user authentication in Korea has experienced new dimensions since December 2020. Accredited certificate, which had been in use for 21 years since 1999, has been abolished. Accredited certificates have provided a trust foundation for various ICT-based industrial developments; however, new changes in the authentication sector are also required due to changes in the service and policy environment. Changes in the service environment occur rapidly because of the emergence of new technologies such as AI, IoT, Bio, Blockchain, and the daily use of non-face-to-face environments caused by COVID-19. Even with changes in the service environment, user authentication remains an essential foundation for providing services. This paper summarizes the current status of user authentication techniques, analyzes major changes in the service environment (such as Metaverse) associated with user authentication, and presents the direction of authentication techniques (Decentralized, Invisible, Privacy-preserving) through the derived implications.

KEYWORDS Authentication, digital identity, DID, metaverse, 전자지갑, CBDC, privacy

Ⅰ. 서론

우리는 온라인과 오프라인에서 하루에도 몇 번씩 본인 확인을 하고 있다. 실제 정당한 사용자인지 확인하는 사용자 인증(Authentication) 절차를 수행하고 있는 것이다. 온라인에서 PC나 스마트폰을 이용하여 은행 사이트(또는 앱)에 접속할 때 ID/패스워드나 인증서 또는 지문 등을 이용하여 본인인증하고, 회사에 출근할 때 사원증을 보여줌으로써 본인인증을 한다. 또한 운전할 때는 운전할 자격이 있음을 증명하기 위하여 운전면허증을 소지한다. 이처럼 인증을 하는 행위는 온라인과 오프라인

* DOI: https://doi.org/10.22648/ETRI.2021.J.360413
* 이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No.2020-0-00321, 5G 서비스 환경에서 프라이버시가 보장되는 자기통제형 분산 디지털 신원 관리 및 보안 기술 개발)

에서 자주 발생한다. 온라인에서 인터넷 초기부터 지금까지 가장 보편적으로 사용하는 사용자 인증 수단은 ID와 패스워드이다. 가장 간단하고 편리한 수단이기 때문이다. 하지만 보안상 취약점 때문에 현재는 OTP, 스마트카드, 바이오, 인증서 등의 다양한 인증 수단이 사용되고 있다. 특히 요즘에는 분실 위험이 없고 편리한 바이오 정보를 이용한 인증 방법에 대한 관심이 높아지고 있다.

1999년「전자서명법」이 발효되고 21년간 사용되었던 공인인증서가 2020년 12월에 폐지되었다. 정확하게는 공인인증서의 우월적 지위를 내려놓고 다양한 인증 수단 중의 하나로 동등한 환경에서 경쟁하게 된 것이다. 이러한 제도적인 큰 변화는 공인인증서가 그동안 관련 ICT 발전에 기여한 바가 큰 것은 사실이지만, 서비스 환경의 변화에 따라 인증 분야도 계속적인 변화가 요구된다는 것을 의미한다. 1990년대 말에 기존의 대면 거래가 인터넷을 기반으로 하는 전자거래로 대체되면서 비대면 인증을 위한 공인인증서 등의 인증 수요가 발생하였다면, COVID-19로 인하여 우리 생활 대부분이 비대면으로 이루어지는 환경으로의 도래는 새로운 인증 수단의 수요가 증가하는 계기가 될 것으로 예상된다. AI, IoT, Bio, Blockchain 등의 새로운 기술의 등장과 COVID-19로 인한 비대면 환경의 일상화 등으로 서비스 환경의 변화가 급속하게 일어나고 있다. 특히, 대면에서 이루어지던 활동들이 온라인으로 급속히 옮겨가고 가상세계에서의 콘서트, 졸업식, 선거 유세 등의 사례들이 생기면서 메타버스(Metaverse)에 대한 관심이 늘어나고 있다.

본고에서는 온라인과 오프라인의 경계가 없는 세상의 도래와 메타버스의 동향에 관하여 살펴보고, 공인인증서의 생성에서 폐지까지의 경과와 새롭게 도래하는 서비스 환경 분석을 통해서 시사점을 도출하고, 이를 통해 사용자 인증기술의 방향성 3가지를 제시하였다.

첫째, 분산화(Decentralized)이다. 사용자 인증은 신뢰체계이다. 인증은 믿을 수 있는 서비스의 제공과 이용을 위하여 정당한 사용자/제공자인지를 확인하는 행위이다. 기존의 중앙집중형(Centralized) 모델은 단순한 구조로 인하여 인증서비스 구축 및 이용이 편리하다는 장점이 있지만, Single-point failure/프라이버시 침해 등과 같은 문제점이 있어, 분산 인증(Decentralized Authentication)에 대한 관심이 높아지고 있다.

둘째, 무형화(Invisible)이다. 기존의 인증 환경은 PC나 스마트폰과 같은 물리적인 인증 수단을 입력할 수 있는 환경이었다. 그러나 IoT 기반으로 공간이 스마트해지면서 환경(공간)이 나를 인증하는 상황이 많아질 것으로 예상된다.

셋째, 프라이버시 보존(Privacy-preserving)이다. AI, Bigdata를 기반으로 하는 Robot(챗봇 서비스 포함) 서비스가 늘어나고 사용자의 취향이나 의도에 맞는 맞춤형 서비스가 늘어나면서 개인정보 침해에 대한 우려도 커질 것으로 보여 프라이버시를 보존하는 기술에 대한 관심이 증가할 것으로 보인다.

본고에서는 Ⅱ장에서 사용자 인증기술의 개요 및 현황을 정리한다. Ⅲ장에서는 향후 서비스 환경의 변화에 대하여 전망해 보고, Ⅳ장에서는 변화된 서비스 환경에서 인증기술의 3가지 방향성을 제시하고 Ⅴ장에서 결론을 맺는다.

Ⅱ. 인증기술 개요 및 현황

1. 인증기술 개요

인증은 상황에 따라 다양한 의미로 사용되고 있으나, 인증(Authentication, 認證)기술이란 다중 사용

자 컴퓨터 시스템 또는 망 운용 시스템에서 시스템이 단말 작동 개시 정보를 확인하는 보안 절차이다. 인증에는 망을 경유해서 컴퓨터에 접속해 오는 사용자가 등록된 사용자인지를 확인하는 것(사용자 인증)과 전송된 메시지가 변조되거나 전와(轉訛)되지 않은 송신자가 보낸 그대로의 것인지를 확인하는 것(메시지 인증)으로 정의되어 있다[1]. 본고에서는 상기 정의 중에서 사용자 인증을 중심으로 기술하였다.

물론 상기의 정의는 서비스 환경에 따라 변경될 수 있다. 즉, 사용자 인증의 경우에 망을 경유해서 컴퓨터에 접속해 오는 사용자라고 정의하고 있는데, 이것은 온라인 환경에서의 인증을 주로 가정한 것이지만 앞으로는 스마트폰 등을 이용하여 집의 대문을 열거나 자동차 문을 열고 시동을 거는 등의 오프라인 상황에서의 사용자 인증으로 확대될 것이다.

사용자 인증 수단은 크게 3가지로 나누어 볼 수 있다. 첫째는 기억에 기반하는 것이다(What you know). 예를 들면, ID/패스워드나 PIN과 같이 사용자가 기억하여 필요시에 입력하는 것이다. 둘째는 소지에 기반하는 것이다(What you have). 예를 들면 OTP(One-Time Password), 보안토큰 등과 같이 사용자가 소지하고 있다는 것을 통해 본인을 증명하는 것이다. 셋째는 본인 자체에 기반하는 것이다(What you are). 지문이나 홍채 등과 같은 사용자의 신체적 특징을 제시하여 본인을 증명하는 것이다.

이러한 구분은 요즘 기술과 서비스 환경의 진보로 세분화되고 있다. 사용자의 생체적 특성에 기반한 바이오 정보 기반은 지문, 홍채 등과 같은 사용자의 신체적 특징을 기반으로 하는 인증과 사용자의 키스트로크, 걸음걸이, 서명 등의 행위적인 특징을 기반으로 하는 인증이 있다[2].

이와 같은 3가지 인증 수단은 절대적인 장·단점이 있다고 보기보다는 각각의 특징을 가지고 있어서 서비스 환경에 맞게 선택적으로 사용하게 된다.

2. 인증기술 현황

가. 공인인증서 폐지와 시사점

국내에서 주요 사용자 인증기술로 언급되었던 것이 공인인증서다. 인증기술의 향후 방향성을 전망하기 위하여 공인인증서의 생성과 폐지까지의 경과를 살펴보고, 시사점을 도출하는 것은 의미가 있다고 본다. 1990년대 말은 인터넷 기반의 다양한 서비스가 나오던 시점이었다. 특히, 이러한 서비스 중에서 인터넷 은행 및 전자상거래 등과 같은 비대면 환경에서 이체 및 결제를 하거나 중요한 계약이 이루어지는 서비스가 증가하기 시작했다. 기존의 대면 상황에서 행해지던 이체나 계약 행위들을 비대면 상황에서 하려다보니 인터넷 건너편에 있는 사람이 정말 현재 계약의 당사자가 맞는지와 그 계약 내용이 위·변조되지 않았음을 확인할 필요가 있었다. 이러한 필요에 따라 만들어진 것이 공인인증서였다.

공인인증서 서비스가 시작된 이후로 인터넷뱅킹, 증권거래, 30만 원 이상의 전자상거래 등에서 의무화되었으며, 2005년에는 1,000만 건 이상이 발급되면서 민간영역뿐만 아니라 연말정산, 나라장터 전자입찰 등의 공공영역까지 사용자 인증이 필요한 분야로 확대 이용되었다[3]. 한국인터넷진흥원(KISA)에 따르면 공인인증서 발급 건수는 지난 2016년 3,544만 건에서 2017년 3,792만 건을 거쳐 2020년 4월 기준으로 4,418만 건에 달한다[4].

1999년 「전자서명법」 제정 및 공인인증서 제도 도입 이후에 민원, 행정, 금융, 전자상거래 등 국가정보화를 촉진함으로써 국민 삶의 질 향상에 기여

하였으나 공인인증서의 우월한 법적 지위로 전자서명 시장의 독점문제를 발생시켰다는 지적을 받아 왔다. 이러한 문제점을 해결하기 위하여 2020년 12월에 정부 주도의 공인인증서 제도 폐지를 골자로 하는「전자서명법」개정의 시행을 통해 다양한 전자서명 수단 간 차별 없는 경쟁 환경을 조성하여 이용자 불편 해소 및 국민의 선택권 확대를 위한 노력이 진행되고 있다[5].

초기에 공인인증서 이용 환경은 유선망에서 PC 기반이었으나 시간이 지나면서 모바일망에서 스마트폰 기반으로 변화되었다.

기술적인 측면에서 서비스 환경 변화에 대하여 기존의 공인인증서가 대응에 한계를 보였던 부분은 다음과 같다.

첫째, 안전성 측면이다. 기존의 공인인증서는 PC의 NPKI 폴더에 파일 형태로 저장되어 있어서, 누구나 접근 가능하여 해킹에 취약할 수 있다는 것이다. 이러한 특징은 NPKI 폴더를 통째로 복사해서 이동식디스크(예, USB)를 꽂은 후 여기에 붙여넣기를 하면 간단하게 복사되어 편리한 부분도 있지만, 악성코드에 의한 해킹에도 취약할 수 있다는 것이다.

둘째, 편의성 측면이다. 기존의 공인인증서를 이용하려면 사용자의 PC에 설치되어 있거나 USB를 휴대하고 다녀야 했다. 또한, PC와 스마트폰에서 이용하려면 별도 복사나 설치를 해야 하는 번거로움이 있었다. 또한 공인인증서를 설치하기 위해서는 Active-X로 되어 있는 다른 보안 관련 프로그램(키보드 보안, 방화벽, 백신 등)을 추가 설치하게 되어 있어 불편할 뿐만 아니라 보안에 취약한 상황을 만든다는 지적을 받아왔다.

셋째, 다양성 측면이다. 민간과 공공영역에서「전자서명법」에 명시되어 있는 공인인증서만을 강제하다보니 바이오, 블록체인 등과 같은 새롭게 등장하는 인증기술이 시장에서 공정한 경쟁이 어려워 사용자들의 선택권을 제한한다는 것이다. 인증은 서비스 수준에 따라 편리성과 안전성을 고려하여 시장에서 결정하여 선택하는 것이 필요한데, 공인인증서만으로 제한하다 보니 사용자의 불편함과 보안상의 취약점이 늘어난다는 지적을 받아온 것이다.

이러한 세 가지(보안성, 편의성, 다양성) 기술적 측면의 시사점은 새로운 환경 변화에서 인증기술의 방향성을 고려할 때 기준으로 참고할 수 있을 것으로 보인다.

나. 민간 인증서 현황

공인인증 제도가 폐지됨에 따라 기존의 공인인증기관인 금융결제원, 코스콤 등의 공동인증서(구 공인인증서) 발급 외에 KB 국민은행, NH 농협은행 등과 같은 개별 은행, 통신 3사나 네이버, 카카오 등과 같은 플랫폼 사업자 등이 인증서 발급 서비스를 하고 있다. 민간에서 발급한 인증서는 서비스 제공자마다 각각의 특징들을 가지고 있지만, 추가적인 프로그램을 설치하지 않고 인증서를 클라우드에 저장하여 스마트폰이나 다른 PC에 별도로 저장·이동할 필요가 없도록 하거나, 지문인증이나 간편 비밀번호 등으로 간편하게 인증할 수 있는 기능을 제공하는 등 기존 공인인증서의 불편한 점을 개선하기 위한 노력을 하고 있다[6].

금년 초에는 국세청 연말정산 간소화 서비스에서 민간 인증서 적용 시범사업을 추진하였다. 다만, 시범서비스에 참여한 KB모바일 인증서, 패스(PASS), 카카오페이 인증서, 삼성패스, NHN페이코 인증서 등 5개 민간인증서보다 공동인증서(구 공인인증서)의 이용이 우세한 것으로 조사되었다. 이것은 아직까지 구 공인인증서의 유효기간이 남아 있고 민간인증서에 대한 인식 부족, 기존 사용

하던 공인인증서에 대한 익숙함 선호, 연말정산에 민간인증서 도입 홍보 부족 등 여러 요인이 작용한 결과로 해석되고 있어 향후 기존 공인인증서의 유효기간 만료와 이용의 편리성에 대한 홍보가 강화되면 민간인증서 이용이 확대될 것으로 기대하고 있다[7].

다. 모바일 신분증 현황

온라인에서 민간기관들에 의하여 다양한 인증수단들이 발급되어 이용되고 있으며, 이러한 움직임은 오프라인으로도 확산되고 있다. 우리 생활의 대부분을 스마트폰에 등록한 신용카드로 결제하다 보니 외출 시에 지갑을 별도로 챙기지 않는 경우가 많은데, 오프라인에서 가끔 필요한 신분 증명을 위하여 신분증이 든 지갑을 별도로 챙기는 것은 여간 불편한 일이 아니다. 이러한 불편함을 해결하기 위하여 스마트폰에 신분증을 탑재하여 실물 신분증을 대체하려는 민간과 공공영역에서의 노력들이 이어지고 있다. 현재 발급되고 있는 모바일 운전면허증은 운전면허 시험장에서 면허증 갱신·재발급 등에 활용되거나 국내선 항공기 탑승 시 신분확인에 사용할 수 있다. 통신 3사의 패스(PASS) 모바일 운전면허증도 제휴를 맺은 편의점(CU·GS25)에서 미성년자 여부의 확인 등 제한적으로 활용되고 있으나, 향후엔 금융이나 보험 등 다양한 분야로 이용이 확대될 수 있을 것으로 전망된다[8].

공공분야에서는 '모바일 공무원증' 구축 사업을 완료하고, 2020년 1월부터 본격적으로 운영을 시작하였다. 모바일 공무원증을 통해 현행 플라스틱 공무원증을 꺼내지 않고도 스마트폰을 이용해 청사 및 스마트워크센터 출입이 가능하고, 행정전자서명(GPKI) 없이도 모바일 공무원증을 이용하여 공직자통합메일 등 업무시스템에 로그인할 수 있다[9]. 행정안전부는 전 국민 누구나 기존 운전면허증과 동일한 효력을 갖는 모바일 운전면허증 서비스를 시작할 예정이고, 모바일 장애인등록증과 외국인등록증도 순차적으로 서비스할 예정이다. 지난해부터 이어진 COVID-19로 비대면·온라인이 일상화되면서 모바일 신분증의 활용은 증가할 것으로 예상된다[10].

이번 공공분야의 모바일 공무원증 도입은 사용자 인증 분야 측면에서 몇 가지 중요한 시사점을 제공한다.

첫째, 온·오프라인 통합이다. 오프라인에서 정부청사 출입을 하기 위하여 보안 게이트 및 사무실 출입 시 사용할 수 있고, 온라인에서 전자결재시스템, 공직자통합메일 등과 같은 공무원 업무시스템 로그인에도 사용할 수 있어 모바일 공무원증 하나로 온라인과 오프라인에서 사용자의 편의성을 높일 것이다.

둘째, 순차적 적용이다. 온·오프라인에서 국민생활의 편의성과 비대면 경제 활성화를 위한 주요 신원 증명 수단으로 모바일 신분증을 도입하려고 한다. 정부는 모바일 공무원증 서비스를 운영하면서 기술적 보완·검증과정을 거친 후, 2021년 말에는 모바일 운전면허증을 전 국민을 대상으로 서비스할 계획으로 단계적 접근을 통해 수용성을 높일 것으로 보인다.

셋째, 모바일 공무원증이 공무원 금융서비스를 위한 e-사람 제증명서(원천징수영수증, 재직증명서, 경력증명서)를 보관 및 제출할 수 있는 기능을 제공하여 신분 증명뿐만 아니라 각종 개인정보를 보관 및 유통할 수 있는 전자지갑의 역할로 확장하겠다는 것이다.

이러한 특징들은 향후 온라인과 오프라인의 경계가 없어지는 세상에서 인증기술의 방향을 전망할 때 참고가 될 수 있다.

Ⅲ. 메타버스 시대의 도래

Microsoft CEO인 사티아 나델란이 COVID-19로 인해 2년이 걸릴 디지털 전환이 2개월 만에 이뤄졌다고 언급한 바와 같이 디지털전환(Digital Transformation)이 급속히 진행되고 있다[11]. 온라인 수업, 화상 회의 및 재택근무 등의 비대면 환경이 한순간에 일상화된 것이다. 우리 생활환경에서 새롭게 부각되는 주요 관심사를 살펴보는 것은 인증기술의 방향성을 전망하는 데 의미가 있을 것이다.

특히, COVID-19로 인하여 기존에 대면에서 이루어지던 생활들이 온라인으로 급속히 옮겨가면서 가상세계에서의 콘서트, 졸업식, 선거 유세 등 사례들이 생기면서 메타버스에 대한 관심이 늘어나고 있다.

1. 메타버스

메타버스(Metaverse)는 현실세계를 나타내는 Universe에 '추상, 가공, 상위의'라는 의미를 가지는 접두어 Meta가 결합한 말로서 풀이하면 '우주 안에 만들어진 의사적인 소우주'를 의미하며, 현실 세계와 같은 사회·경제·문화 활동이 이뤄지는 3차원 가상 세계를 말한다. 그리고 단순한 가상공간이 아니라 가상과 현실이 상호작용하는, 현실에 훨씬 가깝거나 현실보다 더 현실적인 사이버 세상을 말한다[12,13].

2020년 9월 방탄소년단(BTS)은 새 뮤직비디오를 TV나 유튜브 등이 아니라 온라인 게임 '포트나이트' 안에 있는 콘서트장에서 발표하였다. 그 가상공간에 아바타 모습의 세계 각지 팬들이 모여 공연을 관람하고 춤을 따라 추면서 서로 대화하고 즐겼다고 한다[13]. 또한, 네이버 제트의 증강현실(AR) 아바타 서비스인 '제페토' 내에서 진행된 블랙핑크 가상 사인회에는 4,600만 명이 넘는 이용자가 참여하기도 했다[14]. BTS, 블랙핑크 팬들은 단지 화면상에서 보고 즐기는 것을 넘어, 자신도 그 공간에 들어가서 함께 즐기고 생활하는 것이다. 또한 COVID-19로 인하여 실제 졸업식을 할 수 없었던 상황에서 '마인드크래프트'라는 게임 내에서 가상 졸업식을 하는 사례 등이 소개되었다. 메타버스는 비대면·온라인이 일상화된 세상에서 게임·엔터테인먼트 분야에서 시작돼 업무·공공행사 등의 영역으로 확산될 것으로 예상된다[15].

메타버스 등과 같은 가상현실 공간이 일상화되었을 때 사용자 인증과 관련된 요구사항들을 예측해 보면 다음과 같다.

첫째, 새로운 가상공간들이 늘어나면서 우리는 더 많은 다양한 정체성을 가지게 될 것이다. 우리가 현실세계에서도 직장에서의 역할과 가정 및 사회에서의 역할 등이 상황에 따라 구분되듯이 다양한 정체성(Identity)이 존재하게 될 것으로 예상된다.

둘째, 다양한 가상공간에서의 개별적인 정체성을 필요에 따라서 연결하거나 해제하기를 원할 것이다. 즉, 여러 개의 디지털 세계에서 각각 이용하는 ID를 연결하기 위하여 ID연계(Identity Federation)에 대한 자율 조절 기능 요구가 늘어날 것으로 예상된다.

셋째, 가상공간과 현실공간을 넘나드는 환경에서의 편리한 인증 수단에 대한 요구가 늘어날 것이다. 특히, 가상현실 서비스를 위하여 기존의 PC나 스마트폰 환경이 아닌 안경, 헬멧, 슈트 등과 같은 웨어러블 장비를 착용한 상황에서 안전하고 편리하게 인증할 수 있는 방법에 대한 요구사항이 늘어날 것으로 예상된다.

Ⅳ. 인증기술 전망

20여 년 전 공인인증서의 시작에서 현재 폐지에 이르는 과정과 메타버스 등과 같은 온라인과 오프라인의 경계가 희미해지는 서비스 환경 변화를 고려해 볼 때, 향후 인증기술 방향의 주요 특징을 다음과 같이 정리하였다.

1. 분산화(Decentralized)

기존의 중앙 집중화(Centralized)된 인증서비스는 개별 서비스마다 ID/패스워드와 같은 인증정보를 등록하고 기억해야 하는 불편함이 있었다. 이를 해결하기 위하여 통합 인증서비스를 통해 사용자의 불편함을 줄일 수 있었지만, 사용자의 인증정보와 개인정보가 인증서비스 제공기관에 집중됨으로 인해서 개인정보 유출 및 침해 사고 가능성에 대한 우려가 제기되고 있다[16].

유럽의 개인정보보호규정(GDPR: General Data Protection Regulation), 미국의 소비자 프라이버시 권리장전(CCPA: California Consumer Privacy Act) 및 국내 마이데이터 사업 시행 등 개인정보에 대한 주체의 권한 강화 경향이 대두되고 있다. 특히 국내에서도 2020년 데이터3법(개인정보보호법, 정보통신망법, 신용정보법)을 통하여 개인정보 전송권 등과 같은 자기결정권을 강화하고 있다[17].

이러한 경향에 따라 자기주권 신원 증명(Self-Sovereign Identity) 개념이 나오면서 해외에서는 분산식별자(DID: Decentralized Identifier), DID 문서(DID Document)와 신원증명서(VC: Verifiable Credential) 표준화를 진행하는 W3C, 분산ID 상호 연동 및 기술개발을 위한 산업체 연합인 DIF(Decentralized Identity Foundation), 디지털 자기주도 신원증명 오픈소스 프로젝트에 대한 기술지원을 제공하는 비영리 단체 SOVRIN Foundation을 중심으로 연구가 진행되고 있으며, 국내에서는 금융과 통신, IT 분야의 기업들이 참여하고 있는 Initial DID Association과 FIDO Alliance와 금융결제원 등이 함께하는 DID Alliance Korea, 암호화폐 전문기업을 중심으로 관련 개발업체가 연합한 MyID Alliance가 활동하고 있다[18].

다양한 영역에서 분산ID를 접목한 서비스들이 나오고 있다. 한 가지 예를 들면 한 국내통신사는 분산ID 기반으로 고객센터 구비서류 제출을 간소화하는 서비스를 시작했다. 그동안 통신사 고객센터를 통해 업무를 처리할 경우, 각종 신청서 및 구비서류가 필요한 업무는 팩스/이메일로만 제출해야 해서 불편하였는데, 블록체인과 분산 신원 확인(DID: Decentralized Identifier) 기술을 활용해 사용자가 본인 단말에 다양한 증명서를 발급, 저장, 제출하는 서비스로 위변조 및 진위 여부를 검증할 수 있게 하였다[19]. 공공분야에서는 행정안전부의 모바일 공무원증이 FIDO 생체인증과 블록체인 기반 분산ID를 적용하여 보급되고 있다[20].

지갑에 신분증(주민등록증, 운전면허증 등)과 지불수단(신용카드, 할인카드 등) 및 다양한 개인정보(영수증, 진료기록 등)를 보관하고 있다가 필요할 때, 적절한 정보를 선택하여 제출하듯이, 모바일 신분증을 중심으로 소유자의 통제하에 개인정보를 유통할 수 있는 지갑 형태의 기술 등장이 증가할 것으로 예상된다. 특히, 암호화폐 등장 이후에 중앙은행이 발행하는 디지털 법화인 CBDC(Central Bank Digital Currency)에 대한 관심이 높아지면서 전자지갑 기술의 개발 및 실제 적용에 대한 이슈가 늘어날 것으로 예상된다. 여러 개의 ID를 등록하고 이용하기 위해 불편했던 부분은 분산ID 기반의 전자지갑을 중심으로 진화하겠지만 전자지갑의 손·망실로 인한 개인정보 복구 및 위탁 기

술, 전자지갑 이용 편의성을 위한 사용자 경험 기술 및 다양한 도메인에서 추진되고 있는 분산ID를 연계할 수 있는 다중도메인 ID 연계 기술 등에 대한 관심이 증가할 것으로 보인다. 또한, 모든 것이 연결되는 IoT 환경에 적용하기 위한 추가적인 연구가 증가할 것으로 예상된다[16].

2. 무형화(Invisible)

기존의 인증 환경은 PC나 스마트폰 등을 통해 인증 수단을 입력할 수 있는 환경을 주로 가정하였다. 사용자들은 서비스를 이용하기 위하여 키보드로 ID/패스워드나 공인인증서 비밀번호를 입력하거나 스마트폰에서 패턴을 입력하거나 지문인식 장치에 손가락을 가져다 대는 등의 능동적인 행위를 하였다. 이러한 행위는 2가지 측면에서 한계가 있다.

첫째, 안전성 측면이다. ID/패스워드를 이용한 사용자 인증 방법은 패스워드를 잊어버리거나 다른 사람에게 알려주거나 여러 개의 사용자 디바이스와 응용에서 재사용될 수 있는 등의 보안상 문제점이 제시되고 있다. 패스워드의 보안 강도를 높이기 위하여 길거나 복잡하게 패스워드를 생성할 것을 정책적으로 요구하고 있지만, 사용자들은 생성하기 힘들고 기억하기 어려워 기억하기 쉬운 형태로 만들거나 별도로 적어놓으므로 보안에 취약한 부분들이 발생할 수 있다[21].

둘째, 서비스 환경의 변화(편리성) 측면이다. IoT 기술의 확산에 따라 서비스 환경이 스마트화되고 있다. 예를 들어, 자동으로 스마트홈의 전등을 켜고 끄거나 스마트 자동차의 문을 열거나 조작한다면 기존의 키보드를 통한 인증정보 입력 방법으로는 한계가 있을 것이다. 또한, 사용자가 인증한 스마트폰이 타인 혹은 악의적인 사용자에게 탈취되었을 때, 스마트폰 내의 정보 또는 스마트폰을 이용한 제3의 서비스의 불법적인 이용을 막기 위하여 지속인증(Continuous Authentication) 등에 대한 대응도 필요할 것이다[22].

상기의 2가지 한계를 극복하기 위하여 지문, 홍채, 음성 등의 바이오 정보를 이용하려는 시도가 늘어나고 있다. 하지만 패스워드(What you know)나 하드웨어 토큰(What you have) 등과 같은 인증방법과는 다르게, 바이오 인증방법(What you are)은 확률에 의한 인증이라 행위적 특징 기반의 다양한 바이오 인증기술과의 연계를 통하여 사용자의 편의성은 높이면서 보안 수준을 높일 수 있는 다양한 기술들이 소개되고 있다[23]. 특히 이러한 바이오 인증기술은 지식 또는 소유 기반 인증과 연계하는 멀티팩터 또는 두 개 이상의 바이오 인증을 복합적으로 사용하는 멀티모달 방법을 통하여 단일 바이오 인증에 비교하여 FAR(False Accept Rate; 타인수락률: 비인가된 사용자를 인가된 사용자로 인식할 비율), FRR(False Reject Rate; 본인거부율: 인가된 사용자를 비인가된 사용자로 인식할 비율)을 낮추어 줄 것으로 보인다. 예를 들면 키스트록 다이나믹스(Keystroke Dynamics)는 단어의 동일성 여부에 따라 정적(static or structure) 방법과 동적(dynamic or free text) 방법으로 구분할 수 있는데, 정적방법을 활용하여 기존의 비밀번호 기반 인증시스템에 키 입력 특성을 분석하는 키스트로크 다이나믹스 기술을 적용한다면, 입력한 비밀번호가 정확한지 확인한 후에, 비밀번호 각각이 눌리고 해제되는 시간 간격으로 Press-to-Press(PP), Release-to-Release(RR), Release-to-Press(RP) 등의 패턴을 분석하여 추가로 확인한다면 사용자에게 인증을 위한 추가적인 수고 요구 없이 보안성을 높일 수 있을 것이다. 또한 동적 방법을 활용한다면 사용자의 서비스 이용 중에 키스트로크의 패턴 분석을 통하여 지속적으로

정당한 사용자가 이용 중인지를 확인할 수 있을 것이다.

3. 프라이버시 보존(Privacy-preserving)

인증은 정당한 사용자인지를 확인하는 행위이다. 그런데 이 과정에서 프라이버시가 침해될 수 있다.

첫째, 바이오 정보 자체의 특징에 기인한 프라이버시 침해 요인이다. 사용자 인증을 위한 지문, 홍채, 얼굴 등과 같은 바이오 정보는 별도로 기억해야 하거나 휴대해야 하는 불편함이 없고, 타인과 공유되지 않는다는 장점이 있다. 그러나 바이오 정보가 가지는 고유성/불변성으로 인하여, 바이오 정보가 유출된다면 패스워드처럼 재발급할 수 없기 때문에 프라이버시 측면에서 큰 위협이 될 수 있다. 이러한 문제점을 해결하기 위하여 바이오 정보를 서버에 전송하여 저장하지 않고 자신의 단말기에만 저장 및 관리하려는 FIDO와 같은 방법과 바이오 정보 기반의 인증을 위하여 키 정보와 연관(바이오 정보와 결합하여 암호화 키를 숨기거나 바이오 정보를 이용해서 암호화 키를 생성하는 방법)시키거나 다양한 암호학적 도구로 보호(변형함수에 따라 원래의 바이오 정보를 여러 형태로 변형하여 폐기 가능한 바이오 인증방식, 암호화 키로 바이오 정보를 암호화한 상태에서 인증하는 동형암호 방식)하여 인증을 수행하는 방법들이 연구되고 있다[24].

둘째, 서비스에서 필요로 하는 정보 이상의 과도한 정보가 전달되어 프라이버시를 침해하는 경우가 발생할 수 있다. 예를 들어, 편의점에서 주류를 구입하려고 할 때 성인 여부만 밝히면 되는데, 이를 위한 별도의 인증 수단이 없어서 이름, 주소 등의 다양한 개인정보가 기재되어 있는 주민등록증을 제시하여 프라이버시 침해 소지가 있는 경우이다. 또한, 온라인에서는 통합 인증서비스를 이용하여 사용자가 다양한 사이트에 들어가 서비스를 받는데, 통합 인증서비스는 사용자가 어떤 사이트에 접속했는지를 알게 되어 프라이버시 침해가 발생할 수 있다.

향후 사용자가 서비스에 인증을 하는 단계를 지나서 환경이 사용자를 인증하는 스마트서비스 환경이 확대될수록 이런 우려는 늘어날 것이다. 커넥티드 카(CV: Connected Vehicle)의 안전한 운행을 위하여 지속적으로 다른 차량 혹은 기지국과 수행하는 인증을 통해 사용자의 위치정보가 유출될 수 있을 것이다[25]. 또한 사용자의 취향이나 의도에 맞는 맞춤형 서비스를 위하여 AI, Bigdata를 기반으로 하는 Robot(챗봇 서비스포함) 서비스가 늘어나면서 개인정보 침해에 대한 우려도 커질 것으로 보인다. 이러한 우려를 해소하기 위하여 필요한 정보만을 제공해 줄 수 있는 영지식증명기술(Zero-Knowledge Proof)이나 서비스에 따라 필요한 인증 수단을 제공하는 익명인증, 가명인증, 위험기반 인증 등의 기술이 부각될 것이다.

V. 결론

우리나라는 인증분야에 공인인증서라는 의미있는 서비스 경험을 가지고 있다. 1999년부터 20년 넘게 민간과 공공분야에서 널리 쓰이던 공인인증서가 폐지되었다. 정확하게 말하면 폐지라기보다는 '공인'이라는 우월적 지위를 내려놓고 다양한 인증 수단들과 동일한 입장에서 사용자의 선택을 받도록 되었다. 공인인증서에 대한 다양한 긍정적/부정적 의견은 우리의 인증분야에 대한 발전된 안목과도 궤를 같이 한다. 본고에서는 공인인증서가 관련 산업 발전에 기여했음에도 폐지하게 된 이유

를 안전성, 편의성, 다양성 측면에서 분석하고 온라인과 오프라인의 경계가 없어지는 ICT 환경을 알아보고, 이를 통해 향후 인증기술의 방향의 특징을 Decentralized, Invisible, Privacy-preserving으로 제시하였다.

그동안의 공인인증서 서비스 경험은 큰 자산이다. 왜 도입되었는지, 사용 중에 어떤 문제점을 지적받아왔는지에 대하여 검토하여 개선하고 새로운 환경에 적용하려고 노력한다면 우리나라가 현실공간과 가상공간이 융합된 메타버스 환경의 인증분야에서 국제적인 경쟁력을 가질 수 있다고 본다. 앞으로도 ICT 환경은 계속 변화할 것이다. 지속적인 선제적 대응이 필요하다.

용어해설

FIDO(Fast IDentity Online) FIDO는 지문이나 홍채, 음성, 안면 인식 등 생체 인식기술과 USB 보안 토큰, NFC(Near Field Communication) 등 기본 솔루션과 통신표준을 포함한 전 범위의 인증기술을 다룬다.

Metaverse 현실세계를 나타내는 Universe에 '추상, 가공, 상위의'라는 의미를 가지는 접두어 Meta가 결합한 말로서 풀이하면 '우주 안에 만들어진 의사적인 소우주'를 의미하는 현실 세계와 같은 사회·경제·문화 활동이 이뤄지는 3차원 가상 세계를 말한다.

약어 정리

AR	Augmented Reality
FIDO	Fast IDdentity Online
GPKI	Government Public Key Infrastructure
IoT	Internet of Things

참고문헌

[1] TTA, IT용어사전, http://www.tta.or.kr

[2] 사경진 외, "다중 요소 인증에 사용 가능한 행위기반 바이오 인증," 정보보호학회지, 제26권 제6호, 2016, pp. 51-57.

[3] 강효관 "국내 인증기술 및 서비스 현황," 정보보호학회지, 제30권 제3호, pp. 31-36.

[4] 이데일리, "21년만 사라지는 공인인증서 독점…민원서비스도 간편 비밀번호로," 2020. 5. 19.

[5] 국민생활과학기술포럼, "전자서명법 개정과 향후 전망," 2020. 11. 27.

[6] 금융위원회 보도자료, "공인인증제도가 폐지되더라도 금융분야에 편리하고 안전한 인증서가 사용될 수 있도록 하겠습니다." 2020. 12. 9.

[7] 디지털데일리, "연말정산 이용자 대부분 '구 공인인증서' 사용… '민간인증서' 압도한 이유는?," 2021. 2. 24.

[8] 중앙일보, "모바일 운전면허증, 카카오 · 네이버 앱에도 들어간다," 2020. 9. 3.

[9] 행안부 보도자료, "모바일 신분증 시대를 열기 위해 모바일 공무원증 우선 도입," 2021. 1. 13.

[10] SBS Biz, "모바일신분증—행안부 연말 모바일 운전면허증 도입," 2021. 2. 4.

[11] ChosunBiz, "MS 나델라 "2년 걸릴 디지털 전환, 2개월만에 이뤄졌다"," 2020. 5. 20.

[12] 서성은, "메타버스 개발동향과 발전전망 연구," 한국HCI 학회 학술대회, 2008, pp. 600-607.

[13] 경향비즈, "메타버스," 2021. 2. 1.

[14] 매일경제 "미래 선점할 디지털 전쟁터 된 '메타버스'," 2021. 5. 25.

[15] 인사이트, "코로나19로 졸업식 미뤄지자 '마인크래프트'에 모여 가상 졸업한 초등학생들," 2020. 3. 16.

[16] 진승헌 외, "디지털ID관리 기술 현황," IITP 주간기술동향, 2020. 12.

[17] 정중호, "마이데이터 도입과 금융업의 변화," 전자금융과 금융보안, 제23호, 21021-1Q.

[18] 여기호 외, "분산ID보관 및 연계 서비스 모델," 정보보호학회 논문지, vol. 30, no. 3, June 2020.

[19] 디지털투데이, "SKT, 분산ID기반 고객센터 구비서류 제출 간소화 서비스 시작," 2021. 1. 17.

[20] 팍스넷뉴스, "라온시큐어, DID로 공무원증 보급," 2021. 1 .13.

[21] NIST, "NIST special publication 800-63 digital identity guidelines," June 2017.

[22] 조금환 외, "스마트폰 기반 CA기술 동향," 정보보호학회지, 제30권 제5호, 2020. 10.

[23] 김원겸, "행위적 특징 기반 바이오 인증기술 동향," IITP 주간기술동향, 2017. 3.

[24] 박희진 외, "생체인증에서의 프라이버시 보호 기술," 한국정보기술학회논문지, 제16권 제4호, 2018. 4, pp. 109-122.

[25] 정명우 외, "차량익명성을 보장하는 그룹 서명기반 차량용 결제 프로토콜 설계," 한국정보보호학회 논문지, 제29권 제4호, 2019. 8.