The Transactions of the Korea Information Processing Society
TKIPS Vol.14, No.1, pp.41~47

eISSN: 3022-7011
https://doi.org/10.3745/TKIPS.2025.14.1.41

Study on the Failure of DID Service Proliferation: Focusing on the Differences in Perceived Value between Service Providers and Service Consumers

Hwang Hwa Jeong† · Park Min Jung†† · Chai, Sang Mi†††

ABSTRACT

This study aims to provide DID service providers with practical guidance on how to improve DID services. As a result of studying the actual service of providing DID service as a mobile employee card, we found the phenomenon of unmet expectation that the intention of providing the service is not delivered to the service user. It can be argued that DID services are not suitable for mobile employee cards, where the issuer stores all the employees' information, and it can be posited that significant service strategic planning errors lead to the failure of DID service proliferation. We suggest that it is necessary to rethink the service strategy from an ESG perspective, such as trading personal information between companies, rather than replacing the digital version of physical ID cards.

Keywords : Decentralized Identity Services (DID Services), Verifiable Credentials(VC), Data Privacy

DID서비스 확산 실패에 관한 연구: 서비스제공자와 사용자의 인식 차이를 중심으로

황 화 정† · 박 민 정†† · 채 상 미†††

요 약

본 연구는 DID 서비스제공자에게 실질적인 DID서비스 개선 방향 제시에 목적이 있다. DID서비스를 모바일 사원증으로 제공하는 실 서비스를 대상으로 연구한 결과, 서비스 제공 의도가 서비스사용자에게 전달되지 못하는 미충족 기대(unmet expectation) 현상을 발견하였다. 정보 주체가 자신의 정보를 소유, 통제하는 DID서비스는 발급처인 소속사가 모든 사원의 정보를 보유하는 모바일 사원증에는 적합하지 않은 중대한 서비스 기획 오류로 인해 DID서비스 확산을 실패로 유도한다고 판단하며, 물리 신분증의 디지털 버전 대체가 아닌 기업 간 개인정보 거래, ESG 차원의 서비스 전략의 재고가 필요하다고 제언한다.

키워드 : DID서비스, 검증가능한 자격증명(VC), 데이터 프라이버시

1. 서 론

국내외 DID서비스(Decentralized Identity, 분산신원증명 서비스)는 초기 주목받았던 기대와는 달리 현재 관련 기술 및 서비스 확산에 어려움을 겪고 있다. 글로벌 리서치 기관에 따르면, 분산형 ID 시장은 2023년에 10억4천만 달러 규모로[1], 전체 디지털 ID 시장(분산ID, 중앙형 ID, 생체 인증 등 다양한 ID 솔루션 포함)의 동일 기간 279억 달러에 비하면[2], 4% 미만의 시장이다. 이것은 DID서비스가 초기 성장에 대한 예측 대비 현재 보급 수준이 매우 낮음을 보여준다.

DID서비스의 발전은 2015년 미국 국토안보부 과학기술부 '신원 관리를 중심으로 하는 개인정보보호에 대한 블록체인 기술의 적용'이라는 프로젝트 제안을 시작으로[3], 그 핵심기술인 DID가 2022년 7월 W3C에 의해 표준화되기까지 지속적인 진화를 했다[4]. 자기주권신원(Self-Sovereign Identity, 이하 SSI)모델은 블록체인, DID 기술을 활용하여 기존의 중앙집중식 신원인증 모델이 갖는 개인정보 침해와 데이터 유출 등의 한계를 극복한 새로운 패러다임이며, DID서비스는 SSI의 구현체이다[5]. 따라서 DID서비스의 핵심은 정보 주체인 개인의 데이터 프라이버시 보호라 할 수 있다. Westin의 정의에

※ 이 논문은 2024년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임.(NRF-2024S1A5C3A02043653)
† 준 회 원 : 이화여자대학교 경영학과 박사과정
†† 종신회원 : 국립금오공과대학교 경영학과 조교수
††† 종신회원 : 이화여자대학교 경영학부 교수
Manuscript Received : January 3, 2025
Accepted : January 8, 2025
* Corresponding Author : Chai Sang Mi(smchai@ewha.ac.kr)

따르면, 프라이버시는 “개인, 집단 또는 기관이 자신들에 관한 정보가 언제, 어떻게, 어느 정도로 타인에게 전달되는지를 스스로 결정할 수 있는 권리”로[6], 개인의 자기결정권과 자신의 정보에 대한 통제권을 일컫는다. 이 정의는 현대 정보화 시대에서 데이터 프라이버시로 이어졌고, 데이터 프라이버시는 개인의 ‘자기 정보결정권’ 강화와 자기 정보를 능동적으로 ‘통제’할 수 있는 권리로 재구성되었다. 이러한 맥락에서 DID서비스는 기존의 발급자, 검증자가 보유했던 통제의 중심을 개별 사용자로 이동시키는 디지털 시대 신원/자격증명의 해결책이다.

IEEE-ISTO의 Burnett에 따르면, Bhutan 국가 ID(2023년 출시), 스위스 GLEIF 비영리단체의 법인 식별코드, 미국 Privado.ID(구 PolygonID) 등이 있으나[7], 파급력 있게 알려진 사례는 찾아보기 어렵다. 국내에서도 2020년 이후 5개 DID얼라이언스 등 DID 연합체 및 SKT 등 ITC 업체, 라온시큐어, 코인플러그 등 상용화를 위한 노력이 전개되었으나, 열기는 현재까지 지속되지 않고 있다. 일례로, 2020년 범 은행권 블록체인 기반 통합인증서 ‘뱅크아이디(구 뱅크사인)’가 2024년 11월에 서비스를 종료했다. 개별 은행들이 자체 모바일 애플리케이션을 통해 고객 충성도를 강화하고 독점적인 데이터를 확보하려는 전략적 의도가 주요 원인으로 작용하였다[8]. SKT의 이니셜(initial) 서비스는 2020년 이후 모바일 학생증, 전자문서 보관함, 행정안전부 전자증명서 등 다양한 디지털 신원 및 증명 서비스를 지속해서 제공해 왔으나, 시장에서 두드러진 수용이나 성과를 거두지 못했다. 이에 대응하여 2024년 8월, SKT는 구글, 애플, 마이크로소프트와 같은 다국적 기업의 전략을 참고하여 패스키 인증 시스템을 도입함으로써[9], 사용자 편의성 중심의 접근 방식으로 전략을 전환하고 있다. 패스키는 글로벌 표준(W3C, Fido Alliance) 기술로 비밀번호 대신 공개키 암호화 알고리즘을 통해 PC, 스마트폰 등 디바이스가 지원하는 인증방식(생체 인증, 핀 번호 등)을 통해 간편한 로그인과 인증 경험을 제공한다. 전 세계적으로 사용자 편의성을 중심으로 온・오프라인 인증과 기존 디바이스를 대체할 수 있는 보다 간편한 인증 수단의 개발이 활발히 진행되고 있다. 최근 연구 결과에 따르면, 기술기반에 초점을 둔 나머지 기존 SSI 구현은 주로 기반 기술에 초점을 맞추고 종종 사용자 상호작용 측면을 무시한다는 것이 관찰되었다[10]. 요약하면, DID서비스는 초기 관심 대비 실패와 다름없이 정체했고, 전 세계적으로 DID서비스 확산은 중앙집중형의 익숙함과 편리한 대체 수단으로 어려움을 겪고 있다. 본 연구는 인공지능기술의 급속한 발전과 디지털 활동의 폭발적 증가로 데이터 프라이버시 보호의 중요성이 커지는 현시점에서, 현재 국내 DID서비스 연구는 수용 의도 확인 수준으로[11], 실제 사용자 관점의 서비스 경험을 확인한 실용적인 연구는 부족한 실정이다. 본 연구는 이러한 문제의 해결책으로 주목받는 DID서비스가 사회적 확산이 반드시 요구되는 솔루션으로서, 확산 실패 요인 및 확산 촉진 요인에 대해 살펴보고자 한다.

본 연구의 목적은 DID서비스 제공자에게 실질적인 서비스 개선의 방향성을 제시하는 데 있다. 이를 위해 국내 서비스로 DID서비스를 제공하는 서비스제공기업과 도입기업을 대상으로 DID서비스 제공시 제공의도와 전달된 가치를 살펴보고자 한다. 따라서 본 연구는 DID서비스의 확산 실패에 대한 원인을 규명하고, 이에 대한 개선 방향을 제언하고자 한다. 이를 위하여 본 연구에서는 DID서비스에 대한 사용자 경험을 다각도로 접근하기 위해 심층 인터뷰와 설문을 함께 하는 혼합 연구 방식으로 수행한다.

2. 문헌 연구

데이터 프라이버시 보호 기술로서의 DID서비스의 기술현황과 국내외 서비스 현황을 살펴본다. 앞서 제시한 대로, DID서비스는 데이터 프라이버시를 보호해주는 SSI를 구현하기 위해 여러 혁신적 기술을 통합적으로 활용한다. 블록체인 등 분산 원장 기술은 중앙집중식 데이터베이스 대신 분산된 네트워크를 사용하여 데이터의 무결성과 보안을 강화한다. 탈중앙화 식별자(DID)는 사용자가 해당 DID의 소유자임을 증명하여 자신을 인증하는 데 활용되며, 이를 통해 사용자는 중앙기관에 의존하지 않고 자신의 디지털 신원을 직접 통제할 수 있고 관리할 수 있다. 검증가능한 자격증명(Verifiable Credentials, 이하 VC)은 암호화 기술을 활용하여 개인정보의 진위성을 검증하면서도 최소한의 정보만 공개할 수 있게 한다[12]. DID서비스의 이러한 프라이버시 보호 메커니즘은 Mühle et al.등 다수의 연구를 통해서도 확인되어왔다[13]. Guzman-Castillo et al.은 데이터의 프로세싱과 처리, 기밀성과 선택적 정보 공개 및 최소화, 무결성 등이 DID서비스의 데이터 프라이버시 보호를 위한 요구사항임을 확인하였다[14].

DID는 식별대상에 대한 기본적인 정보를 포함하는 전역의 고유식별자이며, 핵심 속성은 영구성, 해석 가능성, 암호학적 검증 가능성, 탈중앙화이다[4]. DID는 ID이므로, 사용자의 신원정보가 아니며, VC에 DID가 연결되어 실제 신원에 대한 증명을 제공한다. VC는 개인의 신원 속성을 신뢰할 수 있는 발급자가 생성하고 서명한 디지털 형식의 자격증명으로, 이는 사용자가 실물 카드 형태로 발급받은 운전면허증이나 회원증과 같은 물리적 자격증명의 디지털 표현이다. VC는 암호학적으로 안전하며 프라이버시를 보존하는 동시에 기계가 검증할 수 있는 방식으로 다양한 디지털 크리덴셜을 제공한다. 이러한 암호화 수단을 통해 위조를 방지할 수 있으며, 타인의 무단 사용 시도를 쉽게 탐지할 수 있는 특징이 있다. VC는 검증자에게 제시되어 자격을 증명하는 데 사용되며, 이를 검증가능한 제시(Verifiable Presentation, VP)라고 한다. 사용자는 발급자가 발급한 VC를 직접 제시하거나, 하나 이상의 VC를 선택적으로 제시할 수 있으며, 특정 정보의 소유를 입증하기 위해 정보 자체를 공개하지 않는 진술 증명도 가능하다.

DID서비스는 W3C와 DIF (Decentralized Identity Foun-

dation), ToIP(Trust over IP), Hyperledger Indy/Aries 등을 중심으로 표준화와 기술적 논의가 활발히 진행 중이다. 해외에서는 비영리단체인 Sovrin 재단과 Indicio 등이 DID 서비스를 위한 메인넷을 구축하여 운영하고 있다. DID서비스의 대표적인 국내 사례는 모바일 신분증이다. 정부는 활용된 블록체인/DID 기술을 활용하여 정보 주체의 자기결정권을 강조하고 있다[15]. 2022년 1월 모바일 운전면허증 도입을 시작으로, 삼성월렛에도 발급할 수 있으며, 2024년 12월 현재 주민등록증을 구축 중이고, 카카오와 네이버 등 민간 월렛에도 발급할 수 있도록 협력 중인 것으로 알려졌다[16]. 국내 DID서비스는 기존의 물리적 신분증(예: 학생증, 사원증)을 디지털 형태로 변환하여, 사용자의 스마트폰에 설치된 디지털 지갑 애플리케이션을 통해 제공되고 있다.

3. 연구 방법

본 연구는 국내 'A' 기업이 개발한 '모바일 사원증' 서비스를 도입한 기업과 서비스 제공 기업을 대상으로 하며, 세 가지 유형의 사용자 그룹을 중심으로 분석을 수행한다. C-Level 담당 임원(급)의 도입의사결정자, 도입한 기업의 서비스사용자와 'A' 기업의 서비스제공자이다.

제이콥 닐슨은 사용성 연구에 따르면, 5명의 표본만으로도 85%의 문제를 도출할 수 있다[17]. 이에 본 연구는 도입의사결정자(5개 기업에서 각 1명, 총 5명), 서비스사용자(13명), 그리고 서비스제공자(5명)로 구성된 총 23명의 세 가지 사용자 집단을 대상으로 평가를 수행하였다. 도입기업은 Table 1과 같으며, 도입의사결정자의 주요 전문 배경을 보면 1명을 제외한 대부분이 IT 업무 경력이 있어, 기술의 이해도가 있음을 확인할 수 있다. 서비스사용자는 인터뷰에 응한 도입기업의 사용자들로, 해당 도입기업 실무자의 협조를 얻어 참여자로 확정하였다. 서비스제공자는 'A' 기업의 모바일 사원증 서비스 기획에서 개발, 제공 업무담당자로, 서비스를 총괄 담당(C-Level), 프로젝트 관리자, 사업 발굴 리더, 응용과 앱 개발 파트장 5명이다.

Table 1. Adopted Company Decision Makers' Overview

Company	Industry	No. of Employee	Key Careers of Adoption Decision Makers
a	Holdings	100	Group/IT Planning, Strategic/Security Expert
b	Medicine Mfg./ Retails	1,300	Sales, Audit, IT Planning
c	System Integration	6,800	IT Solution Planning, System Development
d	Business Education	60	Finance, IT, HR Related Expert
e	System Development	850	HR Planning, Human Resources Management

본 연구 방법은 DID서비스에 대한 사용자 경험을 다각도로 접근하기 위해 심층 인터뷰와 직관적으로 응답할 수 있는 설문조사를 함께 수행하는 혼합 연구 방식을 채택하였다. 인터뷰를 먼저 시행하여 확보한 응답을 바탕으로 설문조사를 수행하였다. 인터뷰는 연구 초기 단계에 문제 확인과 탐색에, 그리고 참여자들의 경험과 인식을 파악하는데 효과적인 방법으로, DID서비스의 현재 확산의 문제점을 확인하는 본 연구에 적합하다고 판단했다. 인터뷰는 사용자들이 경험을 바탕으로 의견을 제시할 수 있도록 Table 2와 같이 개방형 질문을 이용하였다. 인터뷰 질문은 사용하는 DID서비스 사용에 관한 동기, 경험과 데이터 프라이버시를 보호하는 서비스로서의 인식 여부로 구성하였다.

설문 20문항은 1부터 7까지(전혀 그렇지 않다~매우 그렇다) 리커트 척도를 사용하였다. 사용자의 응답에 유의수준 0.001에서 세 집단 간 평균 차이는 통계적으로 유의미한 것으로 나타났다(Table 3).

4. 연구 결과

4.1 심층 인터뷰 결과

모바일 사원증으로 활용할 수 있는 서비스는 도입한 기업에 따라 다소 차이를 보이지만, 일반적으로 오프라인에서는 사옥 출입, 층간 이동, 사원식당, 카페, 편의점, 통근버스 등 복지시설 이용에 사용되며, 온라인에서는 사내 포털 로그인에 활용되고 있다. 대부분 사용자는 모바일 사원증에 대해 긍정

Table 2. Open-ended Questions in-depth interviewees

Category	Open-ended Questions
Q1	How do you feel about your current DID service? (Please compare it to a physical employee ID)
Q2	(to all for each user) Why did you decide to adopt/use/offer DID Service?
Q3	(to Adoption Decision Maker / Service Consumer) How do you feel about storing your ID on your mobile compared to the physical ID card?
Q4	(Before the explanation of DID technology) What is privacy like for you, and is it important to you?
Q5	(After the explanation of DID technology) Do you think the DID service protects your privacy?

Table 3. ANOVA Test Results of User Groups

User Group	M	SD	f	p
Adoption Decision Manger	6.55	0.51	10.3672***	0.0001
Service Consumer	5.93	0.70		
Service Provider	6.32	0.61		

적인 반응을 보였으며, 특히 실물 카드보다 휴대성 측면에서 높은 만족도를 나타냈다. 발급 즉시 실물 사원증과 권한이 연동되어 즉각적으로 사용할 수 있어, 빠르고 편리한 모바일 경험에 긍정적인 평가를 하였다.

모바일 사원증 서비스의 도입과 사용과 제공 목적은 Table 4에서 보는 바와 같이 기업, 사용자, 제공자 등 이해관계자 집단에 따라 다른 양상을 보인다. 모바일 사원증의 도입목적은 기업별로 다양했으며, 이는 'One Company' 전략을 통한 조직문화의 신속한 혁신, 업무환경의 디지털화 추세 반영, 실물 사원증 관리의 보안 취약점 해소 등 기업의 운영 효율성 제고와 디지털 전환 가속화 등의 전략적 접근이다. 서비스사용자들의 이용 동기는 주로 소속 기관이 제공하는 시스템에 대한 순응적 태도에 기인하며, 이는 조직 정책에 대한 수동적 수용의 형태로 나타나는 경향을 보인다. 서비스제공자의 주요 목적은 블록체인과 DID 등 자기주권신원(SSI) 기술을 활용하여, 개인정보 보호에 대한 인식이 높아진 고객층을 대상으로 데이터 프라이버시 보호를 강화한 모바일 서비스를 제공하는 것이었다. 기업의 환경・사회・지배구조(ESG) 책임을 이행하는 차원도 궁극적으로는 가능하리라고 기대하였다.

특히 서비스제공자는 모바일 사원증은 실물 사원증과의 기능적 동등성을 유지하여 기능적 연속성을 보장하고, 사용자 경험의 일관성을 유지하는 것을 핵심 목표로 설정함에 따라, 디자인 요소뿐만 아니라 실용적 기능까지 포괄하는 접근 방식을 취했다. 따라서 서비스 기획 단계에서 출입 통제시스템과의 통합, 그리고 사내외 복지시설과의 연동을 위한 기존 인프라와의 광범위한 연계가 우선순위로 고려되었음이 응답을 통해 확인되었다.

Table 4. The Differences Purposes by User Group

User Group	Purpose of Adoption Decision Making/Using/Service Providing	Keywords
Adoption Decision Maker	• Group/affiliates unified mobile employee ID integration • Manage security, including the risk of lost or misused ID cards • Flexible work arrangements, automated time and attendance records • Employee's digital experience • "Cost of adoption" weighed heavily in decision-making	-Organizational Culture Transformation -Security Risk Reduction -Employee Benefits -Automated Attendance Management
Service Consumer	• Accepted because it's company policy • Recommended from coworkers - portability and curiosity • Eliminated the inconvenience of carrying and passing physical employee IDs	-Passive Acceptance -Curiosity -Portable Convenience
Service Provider	• SSI enabling mobile service offering with innovative new technologies (Blockchain/DID) • Aim to expand business by creating a cost-competitive and digital identity ecosystem with a subscription model	Leading the delivery of privacy innovations technology and fostering the ecosystem

Table 5는 모바일 사원증에 대한 도입의사결정자와 서비스사용자의 프라이버시 관련한 인터뷰 결과이다. 신분증을 실물이 아닌 모바일에 저장하는 것이 프라이버시와 연관하여 어떠한 의견을 갖고 있는가에 관한 질문에 도입의사결정자는 모바일 추세로 익숙하여 이미 결제, 페이를 사용하고 있어 특별히 프라이버시를 고려하지 않는다고 응답하였다. 서비스사용자는 실물 사원증 패용한 사실을 잊은 채 이름/사진을 노출한 상태로 다니는 것보다 모바일에 저장하는 것에 프라이버시 보호한다고 느끼고 있었다. 연구에 참여한 도입의사결정자와 서비스사용자 모두는 프라이버시가 매우 중요하다고 하였다. 프라이버시에 대한 사용자들의 정의는 '나'라는 정체성이자 '나

Table 5. In-depth Interview Results of Privacy Expectations

User Group	Answers
Adotion Decision Makers	• Privacy is important to me, both as a business owner and as an individual. • I think storing IDs on mobile is the way of the future - we already use mobile banking, mobile payments and mobile Pay. • Regardless of whether there are physical passporting rules, both physical and mobile are employee IDs anyway, so it's double management and replacing/investing in access control devices is a real burden to company. • I didn't realize at the time of initial implementation that it was a new technology that protected privacy. I realized it when you explained the solution, but it wasn't a deciding factor. • I don't understand how this solution will help us from a business perspective.
Service Consumer	• Physical cards just need to be touched, but iPhones need to open the app and authenticate, which is annoying, so I don't use them because it's inconvenient. • Privacy... I'm very concerned about my privacy, but I don't do anything about it. I just keep it up to date and don't track my location. • I don't think it's more dangerous to have my ID on my phone, but I have a vague fear that I won't be able to use it if it's compromised by other spam or links. • I care about security and privacy, but having to authenticate multiple times to use a service is so cumbersome and inconvenient that I don't want to use it. • With a physical card, I'd be surprised if I went out for lunch and my name was exposed, but I'm relieved that my mobile is invisible. • I didn't realize this was a new technology and didn't think much about privacy when I used it. • It's good if it's a privacy technology, but I don't have to recommend it. .... • It's an employee ID, and the company already has all my information, so what's the point of me having my own?

의 모든 것', '사생활', '개인정보' 등 다양하였다. 그러나 프라이버시 보호를 위하여 위치추적을 켜지 않거나, OS 업데이트를 수행하는 정도의 조치만을 취한다고 응답하였다. 금융업무 등을 위해 여러 단계의 인증 수행 절차 요구는 불편하고 번거롭다고 응답하여, 프라이버시에 대한 중요성과 실제 보호 행동과의 괴리를 보였다.

서비스사용자 모두 모바일 사원증 서비스가 데이터 프라이버시 보호를 하는 신기술로 개발되었음을 인지하지 못하고 있었다. 기업의 개인정보 보호 활동에 어떤 혜택이 있으며, ESG 차원에서 DID서비스가 어떤 가능성을 제시해주는지 알지 못한다고 응답했다. 특히 모바일 사원증의 개인정보보호 관련한 요인은 서비스의 도입에 어떠한 영향도 주지 않았다는 점이 도입의사결정자들의 공통된 응답이었다.

서비스사용자들에게 모바일 사원증이 개념적, 철학적, 기술적으로 프라이버시를 보호하는 기술이라는 설명을 한 이후에 반응은 매우 긍정적이었다. 회사가 도입한 서비스가 편리할뿐 더러 좋은 기술을 활용하고 있다는 점 때문이었다. 그러나, 이러한 프라이버시 보호 기술이라는 점이 서비스를 도입/사용하지 않는 주변 동료나 타 회사 소속의 기업에 추천이 되겠냐는 점에는 굳이 추천할 이유를 찾지 못한다고 응답하였다. 서비스 사용자들은 모바일 사원증이 소속 회사에서 발급받는 것이고, 소속 회사는 이미 개인의 모든 정보를 보유하고 있는데, 나의 정보를 내가 갖고 주인으로서 통제한다는 것이 어떤 의미를 주는가 하며 연구자에게 반문하였고, 회의적인 반응을 보였다.

이에 본 연구는 두 가지 연구 결과를 도출하였다. 첫째, 서비스제공자의 제공 의도 즉, 데이터 프라이버시에 대한 의도가 서비스사용자에게 충분히 전달되지 못하는 미충족 기대(unmet expectation) 현상[18]을 발견했다. Verinis et al.의 정의에 따르면, unmet expectation은 직원이 미래에 대해 가지는 긍정적 결과에 대한 기대와 실제로 경험하는 성취 수준 사이의 불일치를 의미한다. 서비스제공자는 본래의 제공 의도와 다른 경험 차이의 발생은 그 원인이 서비스 기획이나 전략 차원의 부적합성이 DID서비스 확산 실패의 원인이 될 수 있다고 판단했다. 둘째, DID서비스의 데이터 프라이버시 보호 개념은 도입 의사결정과정과 사용에 직접적인 영향을 주지 않음을 확인했다.

4.2 설문 결과

설문은 유용성과 사용 편리성, 서비스에 대한 신뢰, 프라이버시 관련한 질문이었다. 유용성과 사용 편리성 측면에서는 사용자 그룹 간 유의미한 차이가 관찰되지 않았으나, 서비스 신뢰와 프라이버시 관련 항목에서는 통계적으로 유의한 인식 차이가 확인되었다. 서비스 신뢰와 프라이버시 관련 항목을 분석한 결과, 도입의사결정자와 서비스제공자 간의 인식 차이는 미미한 수준(0.1점)인 반면, 서비스사용자는 이 두 집단과 비교하여 상당한 인식 격차(1.2-1.4점)를 보이는 것으로 나타났다. 이 설문 결과는 인터뷰에서 도출된 발견사항을 뒷받침하여 서비스제공자의 의도가 서비스사용자에게 효과적으로 전달되지 못하는 현상을 실증적으로 재확인함으로써, 제공자와 사용자 간의 인식 격차에 대한 추가적인 증거를 제시한다. 한편, 서비스제공자와 도입의사결정자 간의 인식 유사성이 관찰되었는데, 이는 서비스 도입 및 구축 과정에서 두 집단 간의 상호작용으로 인한 학습 효과로 해석된다. 이러한 과정을 통해 도입의사결정자의 프라이버시에 대한 이해도가 향상된 것으로 나타났다.

5. 결 론

본 연구는 DID서비스를 제공한 서비스제공자와 도입기업 사용자 간의 차이점을 규명함으로써, DID서비스 제공자에게 실질적인 서비스 개선의 방향성을 제시하는 것을 목적으로 하였다. 본 연구는 결론으로 서비스제공자에게 세 가지 확산 촉진 방안을 제시한다. 첫째, DID서비스는 모바일 사원증이라

Table 6. Survey Results by User Groups

Category	Survey Contents	Decision Makers		Service Consumer		Service Provider		f
		M	SD	M	SD	M	SD	
Useful	• Access, payment services • Mobile/digital experiences • Versatile usage	7.00	0.00	6.45	0.26	6.43	0.66	2.25*
Convenience	• Easy and fast to use • Issuance without assistance • Physical vs. mobile convenience	6.26	0.45	6.56	0.23	6.36	0.52	0.69*
Trust	• Trust in the issuance process • Secure information transfer • Counterfeit ability compared to the real thing	6.88	0.16	5.68	0.18	6.80	0.16	68.89***
Privacy	• Ownership/control of my personal data • Selective submission of required information • Physical information exposure	6.70	0.00	5.88	0.10	6.80	0.00	16.5***

*p<0.05, p<0.001, *** p<0.001

는 서비스 기획, 설계 오류로 확산에 실패하고 있다. 서비스제공자는 프라이버시 기술이라고 강조했지만, 사원증으로 서비스를 제공하여, 사용자들은 프라이버시가 보존된다고 느끼지 못한다. 왜냐하면 취업부터 모든 개인정보 제공 및 급여, 평가, 경력 등 모든 정보를 축적하고 있는 기업을 상대로 직원들에게 개인정보의 소유권과 통제권이 본인에게 있는 사원증은 이제는 개인에게 소유나 통제의 대상이 아니기 때문이다. 사원증이라는 신분증이 아닌 기업이 보유한 개인정보를 다루는 관점에서 B2B 거래에 더욱 합리적인 해결 대안으로 접근해야 한다. 예를 들면, B2B 거래 즉, 외부 교육기관에 소속사 인증/검증을 통해 제3기관에 직원 정보의 위 수탁 부담 경감효과와 ESG 경영 차원의 리스크 해결안으로 접근하는 것이다. 개인정보 및 데이터 프라이버시 보호는 사회적 책임과 지속가능성에 직접 연관된 요소이며, 신원 도용, 데이터 유출, 기업평판 등 리스크의 선제적 파악과 대응 전략으로 DID서비스를 기획해야 한다.

둘째, DID서비스 제공자는 사용자들이 해당 서비스를 통해 프라이버시를 보호받고 있다고 인지하도록 사용자인터페이스의 직관성을 높이는 전략을 고려해야 한다. 사용자가 안전한 정보 전송, 검증/사용 기록, 영지식 증명 포함 최소한의 정보 선택 제출 등을 실제 사용 경험에서 시각적인 명료함과 가시성 확보로 서비스 지속 사용을 유도해야 한다. 즉, 사용자 중심의 쉽고 매끈한 UI/UX를 제공하는 방향이 요구된다.

셋째, 서비스(as a service)로 제공시 사용 편이성이라는 실용적인 목적이 고유 목적 보다 우선되므로, 서비스 접근 전략의 재고가 필요하다. 다양한 서비스 사용처 발굴은 물론 기존 실물 카드와 같은 회사 내 출입 용도가 아닌 물리적 공간적 한계 모바일의 편리한 휴대성이 극대화하고, 이 과정에서 사용자의 만족도 및 의견을 조사하여, 기술에 반영하는 선순환적인 피드백 루프가 필요하다.

요약하면, 정부나 서비스제공자들은 DID서비스 기획할 때, 합목적의 서비스 전략과 기획설계 하에 프라이버시 보존기술로서만 강조하기보다는 이를 활용할 수 있는 다양한 사용처 개발과 생태계 확장을 위한 엔터프라이즈의 요구사항과 개인의 요구사항에 기술에 반영하고자 하는 노력을 전개해야 함을 시사한다. 본 연구는 국내 특정 기업의 사례에 한정하여 일반화의 한계가 있다. 연구의 공헌은 DID서비스 제공자에게 DID서비스 기획에 대한 근본적인 질문으로 서비스의 전략적 기획에 대한 통찰력을 제공한다. 본 연구는 DID서비스가 단순한 기술적 솔루션이 아닌 프라이버시와 중요한 개인 신원정보를 다루는 사회적 기술로 정의하고, 생태계 확산의 프레임워크 개발과 중요한 솔루션의 방향성 제시하는 추후 연구로 진행하고자 한다.

References

[1] GMI, "Decentralized Identity Market Size, By Identity Type (Biometrics, Non-Biometrics), By Enterprise Size (Large Enterprise, Small and Medium-sized Enterprises), By Industry Vertical & Forecast, 2024-2032", GMI 10114, 2024.

[2] GMI, "Digital Identity Solution Market - By Component (Solutions, Services), Authentication Type (Single-factor Authentication, Multi-factor Authentication (MFA)), Deployment Mode (On-premises, Cloud-Based), Type, Organization Size, End Use & Forecast, 2023-2032". GMI619.8 2024.

[3] SBIR, "Applicability of Blockchain Technology to Privacy Respecting Identity Management," https://sbir.gov/sbirsearch/detail/867797. 2015.

[4] W3C, https://www.w3.org/TR/did-core/. 2022

[5] A. Preukschat, and D. Reed, "Self-Sovereign Identity," *Manning Publications*. 2022.

[6] A. F. Westin, "Privacy and freedom," *Washington and Lee Law Review*, Vol.25, No.1, pp.166, 1968.

[7] D. Burnett, "Escaping the trap of Identity: W3C VCs and DIDs," *Web3 Conference*, Nov. 2024.

[8] etnews, https://www.etnews.com/20241023000151

[9] SKTelecom, https://news.sktelecom.com/206581

[10] A. Satybaldy, M. S. Ferdous, and M. Nowostawski, "A taxonomy of challenges for self-sovereign identity systems," *IEEE Access*, 2024.

[11] K. S. Lee, "A Study on Distributed Identification (DID): Focusing on the UTAUT model," 2024.

[12] W3C, https://www.w3.org/TR/vc-data-model/. 2024.

[13] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, Vol.30, pp.80-86. 2018.

[14] A. F. Guzman-Castillo, G. Suntaxi, B. N. Flores-Sarango, and D. A. Flores, "Towards designing a privacy-oriented architecture for managing personal identifiable information," *Journal of internet services and information security*, Vol.14, No.1, pp.64-84. 2024.

[15] Ministry of the Interior and Safety, https://mobileid.go.kr/mip/hps/amin.do

[16] https://www.korea.kr/news/policyNewsView.do?newsId=148927211

[17] J. Nielsen and T. K. Landauer, "A mathematical model of the finding of usability problems". In *Proceedings of the INTERACT'93 and CHI'93 conference on Human factors in computing systems,* pp.206-213, 1993.

[18] J. S. Verinis, J. M. Brandsma and C. N. Cofer, "Discrepancy from expectation in relation to affect and motivation: tests of McClelland's hypotheses," *Journal of Personality and Social Psychology*, Vol.9, No.1, pp.47-58, 1968.

황 화 정

https://orcid.org/0009-0001-9537-9089
e-mail : hwajan@ewhain.net
1991년 2월 국민대학교 영어영문학과 졸업(학사)
1999년 8월 서강대학교 경영학과 MBA (석사)
2020년 9월~현 재 이화여자대학교 경영학부 박사과정 MIS 전공
1994년 10월~현재 LG CNS Web3사업팀 책임
관심분야 : 블록체인, 정보보안, 데이터 프라이버시, 탈중앙화 신원증명, Web3, 개인정보보호 등

박 민 정

https://orcid.org/0000-0003-1268-2056
e-mail : mjpark@kumoh.ac.kr
2014년 8월 성신여자대학교 법학과(학사)
2016년 8월 이화여자대학교 빅데이터분석학(석사)
2021년 2월 이화여자대학교 경영학과(박사)
2023년 9월~현 재 국립금오공과대학교 경영학과 조교수
관심분야 : 인공지능, 데이터 애널리틱스 정보보안, 개인정보보호 등

채 상 미

https://orcid.org/0000-0003-4889-7737
e-mail : smchai@ewha.ac.kr
1999년 2월 이화여자대학교(학사)
2002년 8월 서울대학교 경영학과(석사)
2009년 6월 SUNY at Buffalo 경영학 (PhD. 박사)
2012년 3월~현 재 이화여자대학교 경영학부 교수
관심분야 : 인공지능, 블록체인, 디지털 자산, 내부통제, 정보보안, 개인정보보호 등