Trust in the Unknown: Bridging Socio-Technical Gaps in the Trustworthiness of Emerging Electronic Identification Systems

Stepan Bakhaev
Lappeenranta-Lahti University of Technology
Lappeenranta, Finland *stepan.bakhaev@lut.fi*

José Carlos Camposano
Metropolia University of Applied Sciences
Helsinki, Finland *jose.camposano@metropolia.fi*

Annika Wolff
Lappeenranta-Lahti University of Technology
Lappeenranta, Finland *annika.wolff@lut.fi*

Kari Smolander
Lappeenranta-Lahti University of Technology
Lappeenranta, Finland *kari.smolander@lut.fi*

Abstract

This paper analyzes stakeholders' understanding of an electronic identification (e-ID) system based on artificial intelligence and distributed ledger technology. We address the question "How is the trustworthiness of a novel information system for e-ID influenced by the stakeholders' understanding of its base technologies?". Our findings are based on a qualitative analysis of a questionnaire and interviews with stakeholders from a system development project focused on e-ID for online public services. We found that current e-ID systems have good usability but lack dialog and feedback mechanisms, whereas technical robustness and data protection are deemed essential attributes of emerging solutions. We identified four profiles of prospective users according to variations of trust in the new e-ID system. These findings suggest the need for greater transparency to facilitate the adoption of nascent digital identity solutions.

Keywords: electronic identification, stakeholders, trust, socio-technical systems

1. Introduction

Citizens become increasingly dependent on electronic identification (e-ID) to interact with their local or central governments. e-ID is a type of virtual "token" in the form of hardware and/or software that allows an entity (natural or legal person) to be known, through a unique subset of claimed or observed attributes, which are used for the authentication (i.e., corroborating digital identity) and authorization (i.e., granting permission) to gain access to public or private services offered via electronic systems [1]. From the perspective of public administrators, e-ID systems are a part of identity management (IdM) function. They serve as a back-office enabler to guarantee access to digital services, achieve administrative cost savings, and secure cross-border electronic transactions [6], [16].

Even though technology is often the driving force, prerequisite, and key enabler of new solutions, the development of information systems (IS), such as for e-ID, is coupled with challenges related to organizational and social factors [16]. e-ID systems are examples of shared digital infrastructures that emerge from the interactions between various actors who may have different concerns or conflicting interests [3], [16]. For this reason, prior studies have emphasized the need for research that is not limited to the technical aspects [16], but rather investigates e-ID systems as socio-technical artifacts, in which the technical and social aspects are intertwined and inseparable.

Recent advancements in artificial intelligence (AI) have raised the attention of public organizations, because of the opportunities it provides to reduce administrative workload, tackle complex tasks that require making sense of large datasets, and serve citizens faster or in more accessible ways [7]. The growing awareness of challenges, risks, and potential harmful effects of these applications has led to an emerging stream of academic literature and high-level policy guidelines calling for beneficial AI, responsible AI, ethical AI, or trustworthy AI [14], [24]. However, the use of AI in e-ID systems remains a contested area due to the ambiguity of the technology as a "datafier" of existing populations which facilitates undesirable outcomes, such as surveillance and automated decision-making [15].

Furthermore, scientific literature has relied mostly on retrospective case studies of e-ID systems built upon centralized or federated IdM architectures. Research efforts to understand the organizational, social, and legal implications of other types of solutions built upon nascent decentralized or distributed architectures, such as blockchain or distributed ledger technology (DLT) are still limited [23]. Hence, the combination and side-by-side use of DLT with AI has been identified as a promising research direction for the IS community [10], [18], since there is a lack of studies how their convergence impacts the trustworthiness and adoption rate of information systems for e-ID.

We consider that integrating DLT and AI technologies into e-ID systems is not only a technical endeavor. There are social and socio-technical factors related to individual users and the organizational setup of emerging IS, which can have a greater impact on trust and adoption rates than purely technical factors. To understand this better and to address the research gaps, we set the question: *"How is the trustworthiness of a novel information system for e-ID influenced by the stakeholders' understanding of its base technologies?"*. This paper draws on the empirical findings from a stakeholder analysis in the context of an e-ID system development project for online public services. Unlike prior contributions relying on historical case studies of national e-ID implementations [3], [16], we adopt a design-oriented approach to investigate the e-ID system deployed and tested in five different European countries during the four years of the project.

This paper is structured as follows. Section 2 summarizes prior literature related to the base technologies of the studied e-ID system, and their social and ethical implications. Section 3 explains the context of the IS development project and how the proposed solution works. Section 4 describes our data collection methods and the research process. Section 5 presents our key findings and the proposed theoretical framework. Section 6 concludes the paper with the discussion of contribution and implications of our study.

2. Background and Related Research

In this section, we summarize prior research on the base technologies featured in the e-ID system development project. The literature review was initiated at the outset of our research process to provide sufficient base knowledge and complemented *a posteriori*, to enrich the development of theory and the discussion of our findings. It covers two themes related to: (1) the emergence of new e-ID solutions based on DLT and (2) the users' trust in AI and facial recognition. We note that the first theme refers to enabling technology whereas the second theme refers to a social issue of the IS development for e-ID management. Together, these two angles suggest that technical and social factors can both play a key role in the prospective users' willingness and ability to adopt new solutions. The literature on e-ID systems based on DLT describes the technical environment, and the literature on AI and facial recognition describes the social context.

2.1. Technical Angle: Emergence of DLT-based e-ID Systems

There are different types and architectures of e-ID systems, but they can be broadly categorized into independent or isolated, centralized, and federated [1]. In an independent or isolated architecture, each service provider maintains its own user data, or in other words, the e-ID cannot be reused across multiple services because these systems are not integrated. Centralized or federated architectures rely on a single organization or multiple parties, respectively, who act as identity providers in the same trusted domain [4].

The emergence and increasing popularity of cryptocurrencies and DLT since the late

1990's has inspired fresh thinking about the opportunities to design new types of digital identity systems [3], [8]. DLT enables the operation of a highly available, append-only, peer-to-peer database (distributed ledger) in untrustworthy network environments, where separate storage devices (nodes) keep their own local copy of the data that are stored in the ledger [18].

DLT-based e-ID systems represent a departure from prior IdM architectures, because they are designed around the principles of self-sovereign identity (SSI) [22]. This means that an e-ID system runs on a peer-to-peer network, where the digital identity is owned and controlled by the user without the need for an external authority to coordinate the whole network. The emergence of this architectural paradigm has motivated scholars and public administrations to investigate how novel IS for e-ID management can leverage the technical properties of DLT, such as decentralization, transparency, openness, tamper resistance, trustworthiness, cost-effectiveness, and security [21], [23].

2.2. Social Angle: Users' Trust in AI and Facial Recognition

Artificial intelligence is an umbrella concept influenced by many disciplines, such as computer science, business, engineering, mathematics, statistics, and linguistics [26]. It refers to systems based on machine learning (ML) and other algorithmic approaches, which are programmed to self-learn from a given set of objectives and data, in order to make predictions, recommendations, or autonomous decisions on behalf of human beings, thereby solving real-world problems or tasks that are easy for people to perform but difficult to describe formally [18].

Despite the opportunities that AI offers to augment the capabilities of individuals and society, such systems are often considered a "black box", because they rely on algorithms that are inherently complex, continuously adapt to new data, and are difficult to scrutinize [12], [14]. In recent years, an emerging stream of IS literature has called for further studies on the risks and consequences associated to the unintended overuse or the deliberate misuse of AI in the public sector. These ethical issues include the introduction of programmers' biases in the algorithm code or the training data that can influence the AI system's automated decision-making, the target subjects' inability to contest problematic but seemingly plausible results generated by the AI, and the erosion of human self-determination due to the increased reliance or excessive confidence in the AI [12], [14].

Over the last two decades, the use of AI algorithms to deploy biometric systems has raised significant concerns about data privacy [15], [19]. Some of the problems and risks associated with these technologies is the capture of face images without the user being aware of it, the higher probabilities of misidentification among certain groups of people according to their race or ethnicity, the meshing of personal data from different users in group photos, or the fact that deleting a photo does not necessarily remove the user's facial models from the biometric systems' databases. These applications can lead to a paradoxical situation where the e-ID based on biometrics can contribute to enhancing security and at the same time become a threat to privacy.

Trust is a fundamental concept in any IS-enabled situation in which uncertainty prevails or undesirable outcomes are anticipated [13], [24]. It is a complex phenomenon that spans multiple disciplines like sociology, psychology, management, computer science, or IS, but it can be generally understood as the willingness of one entity (A) to become vulnerable and depend on the actions of another entity (B), based on the expectations that B will refrain from opportunistic behavior even under uncertain or risky conditions, and regardless of A's ability to control or monitor B's behavior [1], [9].

Two perspectives on trust have been identified in IS literature: (1) Trust in persons or organizations, and (2) trust in IT artifacts or technologies [13]. Both perspectives (social and technical) are intertwined and relevant for the study of AI-based information systems. In this sense, prior research has focused on three elements that influence the trust and ethical implications of AI: (1) The technical features of the AI that may lead to ethical issues, such as the unchecked collection and storage of personal data; (2) the human factors that may lead to ethical issues, such as the prevalence of race or gender biases; and (3) the interactions among humans and AI in an ethical way, for example during the training of ML models [9], [24].

3. Study Context

The e-ID system featured in our study was a new single sign-on (SSO) solution allowing grassroots citizens or legal representatives of companies to use the camera of their mobile device in order to identify themselves, authenticate, and access online public services. The system incorporated DLT and facial recognition with AI and it was deployed in six pilot sites with different public administrations in five European countries during 2021-2024. Each site featured a unique testing environment and set of user needs listed in Table 1.

Table 1. Overview of the project pilot sites.

Pilot case owner	Public service	Expected value
Municipality in Denmark	Storage of personal documents in municipal lockers	Accessibility and safety of services for vulnerable citizens
Regional police unit in Spain	Filing crime complaints via the police portal	Facilitating operational workflow for police investigations
Municipality in Spain	Online public services available in the city web application	Introducing new method of user authentication in the app
Municipality in Bulgaria	Digital services of the state e-government agency	Usability and reliability of digital services with the new e-ID methods
Municipality in Iceland	Online forum for discussions of citizen initiatives	Engaging citizens with physical disabilities in public discussions
Digital business register office in Italy	Access and management of organizations' fiscal documentation	Increasing accounting controls and reliability with organizational e-ID

To register and create a new e-ID (i.e., "user onboarding"), the user was requested to present an identification (ID) document and to take a live picture of their face. This document, which could be a passport or any other type of legally recognized national ID, had to be held in front of the device camera. After the ID document was scanned, the person took the photo of their face (a "selfie"). Based on these inputs, the software applied a combination of AI algorithms using biometrics and document verification techniques. This involved checking the validity of the ID document (document verification) and determining whether the photo in the ID document matched the real-time picture of the person holding it (facial recognition).

Provided that the verification was correct, a derived e-ID was registered in a private blockchain managed by a distributed network of nodes. Identities stored on this distributed ledger (blockchain) were not under the control of any single organization participating in the project. Instead, the citizen retained control of their own e-ID, associated personal information, and the rules enforcing the informed consent clauses for processing such data. The user's e-ID was stored in the user's own mobile device in the form of a "verifiable credential", containing a pair of public and private cryptographic keys. Only the public key was stored in the distributed ledger to serve later as proof of integrity for the e-ID.

Whenever the user requested access to a public service, they could simply authenticate with the newly derived e-ID. The public administration compared the public key from the user's mobile credential with the public key stored in the blockchain and then requested the user to prove their identity again by issuing a new biometric challenge. If the real-time facial recognition process resulted in a perfect match, the identity was approved, and the user was granted access to the requested online service.

4. Research Process

The findings of this paper are the result of a qualitative analysis of primary data obtained from the meetings with the representatives of the six pilot cases, an online questionnaire, and semi-structured interviews with the project stakeholders. Figure 1 shows an overview of the research process. Our choice of a research strategy was motivated by the attempt to secure a holistic understanding of trust in the new e-ID system developed in the context of the project. Based on the guidelines for conducting mixed methods research, we employed the sequential approach to facilitate the development of our theoretical perspective and augment the insights from each iteration [25]. We describe these iterations in this section.

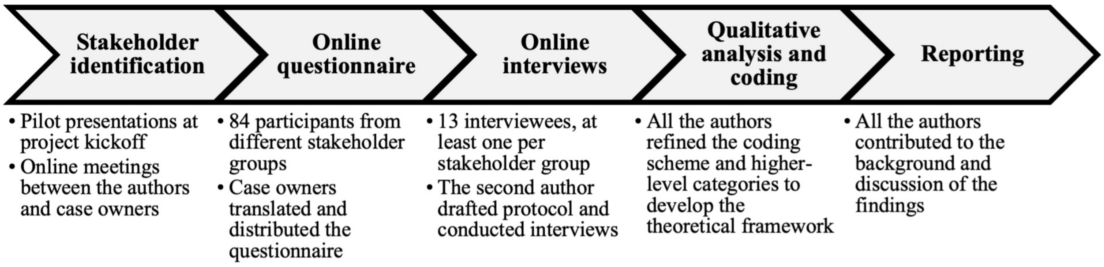
Stakeholder identification
Online questionnaire
Online interviews
Qualitative analysis and coding
Reporting
• Pilot presentations at project kickoff
• Online meetings between the authors and case owners
• 84 participants from different stakeholder groups
• Case owners translated and distributed the questionnaire
• 13 interviewees, at least one per stakeholder group
• The second author drafted protocol and conducted interviews
• All the authors refined the coding scheme and higher-level categories to develop the theoretical framework
• All the authors contributed to the background and discussion of the findings

Fig. 1. Overview of the research process.

4.1. Stakeholder Identification

At the beginning of the project, we set to provide the case owners with detailed guidance and a template to identify the most relevant stakeholders in their pilot sites. We asked them to discuss within their teams and reflect on the different groups of stakeholders, both internal and external to the public administrations, who had to be involved in the pilot cases for the new e-ID system. These stakeholder roles were based upon prior literature on requirements engineering [2] and comprised citizens (end-users), financial sponsors, regulators and policymakers, external advisors/consultants, software developers and vendors, among others. The case owners contacted at least one person per each stakeholder category and invited them to fill in the questionnaire described in the next subsection. Due to the COVID-19 pandemic, the questionnaire was conducted online.

4.2. Online Questionnaire

The questionnaire largely contained closed questions with a predefined and standardized response format, to facilitate the cross-case analysis and comparisons [11]. There were two blocks of questions. The first block was aimed at the stakeholders' prior experiences with current e-ID systems and how well they meet their expectations in terms of software quality attributes. The second block referred to how important would be for participants to find those same software quality attributes in the new e-ID system.

The questionnaire was translated into the local language of each pilot site with the help of case owners, to avoid misunderstandings and encourage participation. In total, 94 people opened the questionnaire invitation link. We collected 84 valid responses (an 89,36% completion rate among those who opened the link), while the remaining 10 participants declined the Privacy Notice and Consent Form. All participants were older than 18 years, and the majority (77%) were familiar with the online public service in their respective pilot site. The share of participants from each pilot case was between 14% and 19%.

4.3. Semi-Structured Interviews

Out of the 84 valid responses to the questionnaire, 39 respondents agreed to be invited for a follow-up interview, and 13 participants (2-3 per pilot case) scheduled an interview with the second author. All interviewees were adults aged 18-60 years from either gender, currently employed, and with at least secondary level of education. The interviews were semi-structured with a duration of 30-45 minutes and relied on a protocol containing close- and open-ended questions, which were scripted beforehand but not necessarily asked in the same order [17]. This method allowed to collect unscripted answers from the participants and to keep consistency among interviews. All stakeholders were individually interviewed and gave their consent to record the conversation for subsequent analysis.

4.4. Qualitative Analysis and Coding

The coding techniques used in the qualitative analysis of our primary data were: Process coding (i.e., actions expressed with "-ing" gerunds, in order to synthesize antecedents, causes, and consequences); open coding (i.e., searching for patterns of relations, similarities, and differences among the respondents); and in-vivo coding (i.e., summarizing the intended meanings of the participants' answers by using their own words) [5], [20]. Some examples of the initial codes identified with each technique were: *"Understanding how AI and blockchain work"* (process), *"Prior experience with AI and facial recognition applications"* (open), *"Blockchain is a black box or misunderstood"* (open), and *"There are too many passwords and usernames I have to remember"* (i.e., = the impracticality of lacking an integrated e-ID solution, in-vivo). The authors collaborated in the development of the higher-level categories and agreed on a framework to answer the proposed research question, based on the review of literature about the technical and social angles of the IS development for e-ID (Section 2). We present the results of our qualitative analysis in the next section and our theoretical contribution in Table 2.

5. Findings

5.1. Stakeholders' Understanding of the e-ID System Base Technologies

Throughout the six pilot cases, most participants agreed that the current e-ID systems were efficient and easy to use. However, the reliability and the quality of instructions or feedback provided by these e-ID systems usually received the lowest scores among the software quality attributes listed in the questionnaire. When stakeholders were asked what quality attributes of the new e-ID system would be most important to them, questionnaire respondents gave the highest priority to privacy/protection of personal data and technical reliability/robustness (Figure 2). No significant variations in the answers were observed among the six pilot cases.

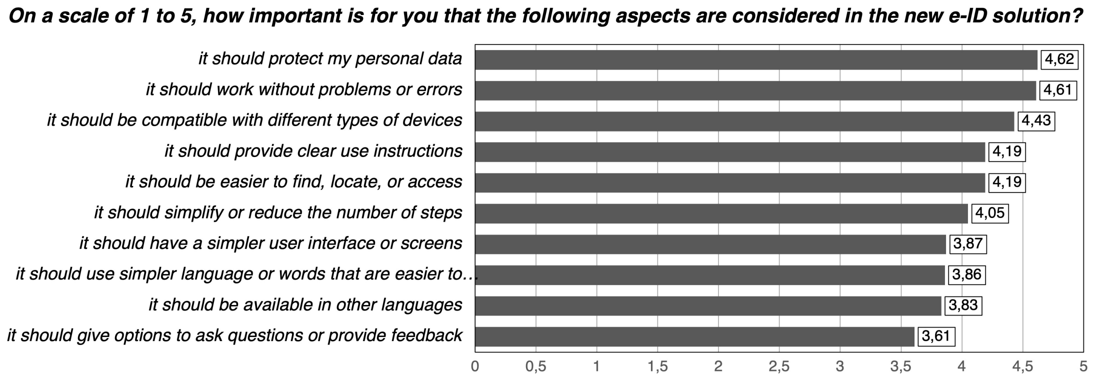

Fig. 2. Most important attributes of the new e-ID system according to survey respondents.

Similarly, interviewees across all pilot cases replied that they would be more likely to trust the novel e-ID system if they knew who would manage their personal details, and how the risks of leakage, theft, or misuse of data would be mitigated in the new system. Interviewees were also in favor of new solutions based on SSI that could allow them to keep control of the information stored in their devices:

> *"-This all [new e-ID system] sounds fantastic to me. For example, right now I unlock my phone using the fingerprint and it's way more convenient than entering a password [...] the concerning part for me is where is that information going to be stored, whether it is going to be stored directly in my phone, encrypted and non-reusable, or if the objective is to store it in some system to make it reusable, I would then expect it is [hosted by] a trustworthy organization." – Head of department, local government*

In terms of familiarity with the base technologies of the system, participants had more knowledge about facial recognition or AI than about DLT or blockchain. In the latter case, most of the answers were some variations of *"Sorry, I don't know what blockchain is or how it works,"* whereas in the former case most interviewees were even able to give examples of applications in which they have observed the use of AI and facial recognition. We observed that prior knowledge elicited different types of reactions. On the one hand, participants with a stronger technical background (e.g., due to their current job position) or that had received more information about the proposed e-ID system seemed skeptical about testing new AI applications that could recognize a citizen’s identity from face photos:

> *“-I’ve seen this [facial recognition] in a movie and it caught [my attention] very much, but then then what’s behind it in terms of ethics and GDPR? […] Where is the information going? Just to protect myself and be sure that this information is not shared somewhere or used in another way [different than] the purpose it has been aimed in the beginning.” – Project manager, local government*

On the other hand, stakeholders that had less prior knowledge or were less informed about AI in the proposed e-ID system as a whole were still enthusiastic, but at the same time, they seemed unaware of the possible risks and consequences of facial recognition:

> *“I use it [facial recognition] on the iPhone every day, [it works] even if I have sunglasses on, I’m very comfortable with it and it feels very secure” – Public servant, local government*

5.2. Stakeholders’ Trust in a Novel e-ID System

We identified two key dimensions of *trust* in the new e-ID system, a central category that emerged across the variations observed in the interviews and questionnaire responses. The first dimension is *technological trust* which is characterized by the stakeholders’ prior knowledge or proficiency in using the underlying technologies of the proposed e-ID solution. This trust stems from the technical properties of the e-ID system and stakeholders’ intentions for the technology, such as the selective presentation of personal information (using verifiable credentials), or the completeness of electronic transactions. The second dimension is *institutional trust* which precedes the use of the e-ID system due to its symbolic (social) properties. This trust varies in stakeholders’ acceptance, or willingness to use such technologies in their everyday life because the trustworthiness of the new e-ID system was tied to the transparency or inclusivity of institutions and their practices based on the system’s outcomes.

This convergence of social and technical aspects allowed us to discern trust as a key factor in the adoption of novel information systems for e-ID. Based on the differences identified in stakeholders’ trust and variations in software quality attributes for the e-ID system, we broadly characterized potential users of a novel IS into the four types of profiles in Table 2. Each one of these four user profiles requires different types of engagement, focusing for example on fostering dialog and feedback with *‘sceptic’* users, or in providing more training and support to *‘enthusiast’* users. Additional interventions must be arranged to help the most *vulnerable users*, who belong to segments of the population that might be excluded or marginalized from adopting a new IS for e-ID. Even if such a solution may be less complex, friendlier, or easier to use (e.g., the proposed e-ID system only required the user to have a smartphone without the need for any additional card readers, tokens, PINs, or passwords), the adoption might still be hindered by the users’ simultaneous lack of technical expertise and institution-based trust in technologies, such as AI or DLT. The aim is to guide everyone toward the upper right quadrant of Table 2, to help them become enthusiastic “keystone” actors in emerging IS that can compel others to join.

Table 2. Four profiles of the prospective users of a novel information system for e-ID.

Stakeholders’ relationships with the e-ID system base technologies		**Institutional trust**	
		Lower transparency or inclusivity	**Higher transparency or inclusivity**
Technological trust	**Higher proficiency or prior knowledge**	Experienced hesitant (“sceptic”) ➔ Conflict: Users that need more reassurances/dialog or whose concerns need to be addressed, in order to adopt the system	Experienced confident (“adopter”) ➔ Target: Users who will adopt the system on their own and can act as ambassadors or promoters
	Lower proficiency or prior knowledge	Novice hesitant (“vulnerable”) ➔ Risk: Users with increased information needs or traditionally marginalized, who are unable to adopt the system on their own	Novice confident (“enthusiast”) ➔ Potential: Users that need guidance/facilitation or whose skills need to be developed, in order to adopt the system

6. Discussion and Conclusions

Recent developments in e-ID systems have primarily focused on establishing trust through their technical design and implementation [22]. However, this has also brought challenges related to data privacy and inclusivity of novel systems [15], [27]. IS scholars have emphasized the need for more research that can bring the technical and social perspectives together to guide system developers in dealing with these challenges, which have a socio-technical, organizational, and managerial nature [16]. In response to this call, we set to answer the research question *"How is the trustworthiness of a novel information system for e-ID influenced by the stakeholders' understanding of its base technologies?"*. Based on the findings of our study, we argue that trust must be approached as a multidimensional concept because it is tightly linked to the institutional properties of e-ID systems along with their technological base.

We contribute to prior studies by proposing the theoretical framework based on the dimensions of *technological* and *institutional trust* (Table 2) with the aim to facilitate the adoption of new IS for electronic identification when new or unknown technologies, like AI and DLT, underpin their functional design. To facilitate the adoption of novel solutions, the specification of software requirements as well as the choice of dissemination and design activities must be tailored to the distinct needs and points of view of *sceptic*, *enthusiast*, and *vulnerable users*. Our findings suggest an opportunity to improve the clarity and transparency of e-ID systems, as many stakeholders do not fully understand how they work or lack feedback mechanisms to voice their concerns. Therefore, the development of future solutions should focus on the institutional as well as technical properties of e-ID systems [27] to provide new channels and mechanisms for user involvement and to promote dialog among stakeholders of emerging IS.

Our study has important implications for practice. The assessment of prospective user-adopters according to the technological and institutional dimensions of trust helps bring attention to the active role that both the system developers and the public administrations alike play in reducing inequalities and increasing the trustworthiness of their solutions. According to our research results, the potential benefits of DLT, such as decentralization, enhanced security, or cost-effectiveness, [21], [23] cannot be fully leveraged if the users do not even understand in the first place what DLT is or how it works. We argue that (social) fairness and (technical) transparency are two key enablers of trust in emerging IS for e-ID, especially those that remain bound to strict regulations and unclear user expectations [27].

One of the main limitations of our study is that it relies on the findings obtained in the system development project focused on e-ID for online public services. We recognize the greater extent of ongoing initiatives in the development of IS for electronic identification which involve public-private arrangements [6]. Therefore, future research could refine and validate the proposed framework further with a larger pool of prospective users including those using services provided by private organizations.

Acknowledgements

This research was supported by the project funded by the European Union's Horizon 2020 research and innovation program under grant agreement No 101004459.

References

1. Alpár, G., Hoepman, J.-H., Siljee, J.: The Identity Crisis Security, Privacy and Usability Issues in Identity Management. 15 (2011)
2. Ballejos, L.C., Montagna, J.M.: Method for stakeholder identification in interorganizational environments. Requirements Eng. 13 (4), 281–297 (2008)
3. Bazarhanova, A., Magnusson, J., Lindman, J., Chou, E., Nilsson, A.: Blockchain-Based Electronic Identification: Cross-Country Comparison of Six Design Choices. In: Twenty-Seventh European Conference on Information Systems. (2019)
4. Carretero, J., Izquierdo-Moreno, G., Vasile-Cabezas, M., Garcia-Blas, J.: Federated Identity Architecture of the European eID System. IEEE Access. 6 75302–75326 (2018)

5. Corbin, J., Strauss, A.L.: Basics of qualitative research: techniques and procedures for developing grounded theory. Sage, Los Angeles (CA) (2008)

6. Degen, K., Teubner, T.: Wallet wars or digital public infrastructure? Orchestrating a digital identity data ecosystem from a government perspective. Electron Markets. 34 (1), 50 (2024)

7. Drobotowicz, K., Kauppinen, M., Kujala, S.: Trustworthy AI Services in the Public Sector: What Are Citizens Saying About It? In: Dalpiaz, F. and Spoletini, P. (eds.) Requirements Engineering: Foundation for Software Quality. pp. 99–115. Springer International Publishing, Cham (2021)

8. Dunphy, P., Petitcolas, F.A.P.: A First Look at Identity Management Schemes on the Blockchain. IEEE Security & Privacy. 16 (4), 20–29 (2018)

9. Hoff, K.A., Bashir, M.: Trust in Automation: Integrating Empirical Evidence on Factors That Influence Trust. Hum Factors. 57 (3), 407–434 (2015)

10. Karger, E.: Combining Blockchain and Artificial Intelligence – Literature Review and State of the Art. In: Forty-First International Conference on Information Systems. p. 18. (2020)

11. Kitchenham, B.A., Pfleeger, S.L.: Principles of survey research: part 3: constructing a survey instrument. SIGSOFT Softw. Eng. Notes. 27 (2), 20–24 (2002)

12. Kronblad, C., Essén, A., Mähring, M.: When Justice is Blind to Algorithms: Multilayered Blackboxing of Algorithmic Decision Making in the Public Sector. MIS Quarterly. 48 (4), 1637–1662 (2024)

13. Lankton, N.K., McKnight, D.H., Tripp, J.: Technology, Humanness, and Trust: Rethinking Trust in Technology. Journal of the Association for Information Systems. 16 (10), 880–918 (2015)

15. Lockey, S., Gillespie, N., Holm, D., Someh, I.A.: A Review of Trust in Artificial Intelligence: Challenges, Vulnerabilities and Future Directions. In: Proceedings of the 54th Hawaii International Conference on System Sciences (HICSS). (2021)

15. Masiero, S., Arvidsson, V.: Degenerative outcomes of digital identity platforms for development. Information Systems Journal. 31 (6), 903–928 (2021)

16. Melin, U., Axelsson, K., Söderström, F.: Managing the development of e-ID in a public e-service context: Challenges and path dependencies from a life-cycle perspective. TG. 10 (1), 72–98 (2016)

17. Myers, M.D., Newman, M.: The qualitative interview in IS research: Examining the craft. Information and Organization. 17 (1), 2–26 (2007)

18. Pandl, K.D., Thiebes, S., Schmidt-Kraepelin, M., Sunyaev, A.: On the Convergence of Artificial Intelligence and Distributed Ledger Technology: A Scoping Review and Future Research Agenda. IEEE Access. 8 57075–57095 (2020)

19. van der Ploeg, I.: Written on the body. Computers and Society. (1999)

20. Saldaña, J.: The coding manual for qualitative researchers. Sage, Los Angeles (2013)

21. Schlatt, V., Sedlmeir, J., Feulner, S., Urbach, N.: Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. Information & Management. 59 (7), 103553 (2022)

23. Sedlmeir, J., Huber, J., Barbereau, T.J., Weigl, L., Roth, T.: Transition pathways towards design principles of self-sovereign identity. In: Proceedings of the 43rd International Conference on Information Systems (ICIS). (2022)

23. Sedlmeir, J., Lautenschlager, J., Fridgen, G., Urbach, N.: The transparency challenge of blockchain in organizations. Electron Markets. 32 (3), 1779–1794 (2022)

24. Thiebes, S., Lins, S., Sunyaev, A.: Trustworthy artificial intelligence. Electron Markets. 31 (2), 447–464 (2021)

25. Venkatesh, V., Brown, S.A., Bala, H.: Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems. MISQ. 37 (1), 21–54 (2013)

26. Wang, W., Siau, K.: Ethical and Moral Issues with AI. In: Twenty-fourth Americas Conference on Information Systems. p. 6. (2018)

27. Weigl, L., Barbereau, T., Fridgen, G.: The construction of self-sovereign identity: Extending the interpretive flexibility of technology towards institutions. Government Information Quarterly. 40 (4), 101873 (2023)