Onboarding Citizens to Digital Identity Systems

Tasos Spiliotopoulos[1*], Al Tariq Sheik[2], Debora Gottardello[3], and Robert Dover[4]

[1]*School of Computer Science, University of Birmingham, Birmingham, UK*
[2]*The Alan Turing Institute, London, UK*
[3]*Edinburgh Business School, University of Edinburgh, Edinburgh, UK*
[4]*School of Criminology, Sociology and Policing, University of Hull, Hull, UK*
[*]*Email: a.spiliotopoulos@bham.ac.uk*

Abstract

Digital Identity (DI) technologies have the potential to enhance the quality of life of citizens through the provision of seamless services, improve the effectiveness of public services, and increase overall economic competitiveness. However, lack of access to DIs can limit these benefits, while unequal access can lead to uneven distribution of these benefits across social groups and escalate existing tensions. Accessible, user-friendly and efficient onboarding can play a key role in ensuring equitable access and wide adoption of DI technologies. This paper proposes the development of physical locations (Experience Centres) that can be used for citizen onboarding to national DI systems, positively shaping citizens' first impression with the technology and, in turn, promoting adoption. To this end, we outline a multidisciplinary research approach for identifying and addressing the considerations necessary for designing, developing and operating a model Experience Centre for DI onboarding in an inclusive manner.

1 Introduction

In recent years, policymakers, researchers, and practitioners around the globe have recognised the potential benefits of Digital Identity (DI) systems [1]. Governments have begun implementing digital identity programmes to provide legal and regulated digital identities to citizens. The UK government has taken a large step in this direction by publishing a beta version of the *Digital Identity and Attributes Trust Framework* [2], which is intended to provide a policy framework that enables and encourages the ability for individuals to have reusable certified Digital IDs.

DIs provide citizens with easy, efficient, privacy-preserving and secure access to services. This, in turn, allows governments and businesses to innovate, streamline their services, comply with regulations and compete at the international level. For example, researchers have highlighted how the selective disclosure and self sovereignty afforded by DI technologies can address financial exclusion [3, 4], while also supporting innovation [5].

Despite the potential advantages, research indicates that the design and implementation of national DI systems may have significant socio-economic, ethical, privacy, and human rights implications [6]. When designing and implementing DI systems, these implications must be carefully considered, as they have the potential to affect a wide variety of individuals and groups. One important consideration involves the onboarding process, which needs to be designed in a way that promotes equitable access to DIs for all citizens. This paper outlines a research approach for identifying and addressing the considerations necessary for designing, developing and operating a physical location (an Experience Centre) for DI onboarding in an inclusive manner.

2 Digital Identity Technologies

2.1 Technical Background

In broad terms, a digital identity refers to what an entity, object or subject is [7]. A key characteristic of a digital identity is that it can be used to prove something about an entity. This means that a third entity can verify a claim that an issuer of the identity has made about the identity holder. This, in turn, means that services and organisations can trust these claims. With this in mind, Kameron [8] has defined a digital identity as 'a set of claims made by one digital subject about itself or another digital subject'. When considering identities at the national level, the UK Digital Identity and Attributes Trust Framework refers to a DI as a 'digital representation of a person acting as an individual or as a representative of an organisation' and highlights the importance of the ability for people to prove claims about themselves and the impact that this foundation of trust can have on organisations, service providers and the country's economy [2].

A DI *system* is a mechanism that permits the creation and verification of an individual's identity using digital means. The process of using an identity within this system consists primarily of two steps: (i) onboarding, and (ii) authentication and ID management. During the initial phase of the onboarding procedure, an individual's Personal Identifiable Information (PII) is collected, validated and verified. This information is used to identify and establish the user within the system. Document validation, email verification, and phone verification may be included in the de-duplication and verification process. Once the individual's identity has been proven, the administrator facilitates in creating an identity record. The second stage of the process is authentication and ID management, in which the individual's identity is verified and man-

aged whenever they attempt to use a service. This is achieved through a variety of methods, including password-based authentication, two-factor authentication, biometric authentication, issuing, recording credential, binding, expiration, renewal and revocation. The authentication phase's objective is to ensure that only authorised users can access the service and their credentials are managed.

2.2 Policy Background

The UK Digital Identity and Attributes Trust Framework (DIATF) provides a preliminary and evolving set of rules and standards for those providing (or independently certifying) DIs. The DI providers will need to follow these rules and standards in order to provide secure and trustworthy digital identity and attribute solutions in the UK market. The drafting of the DIATF is being overseen by the UK government's Department for Digital, Culture, Media and Sport (DCMS), but this process involves a number of government, scientific, policy and corporate stakeholders injecting expertise into the process. At the time of writing there is no definitive publication date for the final version of the DIATF, with the DCMS stating that it will be published in the short term. However, the currently published beta version makes clear the government's intention to use the trust framework to enable services such as digital right to work, rent and criminal record checks [2].

The DIATF is an important element of the UK government's digital economy initiatives that they argue will facilitate increased levels of innovation, competition, and transparency into the digital identity market. The initial DIATF also puts special emphasis on the protection of individual privacy and security. Such ambitions are tempered by the government's parallel policy agenda of deanonymising individuals to improve the work and effectiveness of law enforcement and intelligence agencies.

The transnationality of digital markets sits uneasily with Westphalian constructs of sovereignty, and so the DIATF will need to be compatible (in important ways) with the European Union's proposed European Digital Identity Framework [9], which builds on the existing cross-border legal framework for trusted digital identities, the European electronic identification and trust services initiative (eIDAS Regulation) [10].

2.3 Considerations around Access to DI Technologies

DI systems, when not designed appropriately, may fail to address the needs of those who already carry significant markers of social and economic marginalisation. Such exclusion results in negative economic consequences and serves to further exclude them from formal mechanisms based upon trustworthy identity systems. For example, biometric identification methods, such as fingerprints, may not be accessible to disabled or elderly individuals, creating 'digital barriers' to access economic and social resources [11, 12]. Additionally, digital identification may enable more efficient discrimination against marginalised groups, such as women, ethnic minorities, religious groups, disabled individuals, and members of the LGBT community [13]. These systems also pose a threat to personal safety of marginalised groups. Therefore, more trustworthy digital identity systems that address the rights of all individuals, particularly the most marginalised, will be necessary in the future.

Research has shown that in the UK, around 11 million people especially from marginalised backgrounds do not have a passport or a driving licence. Women, those living in urban areas, the under 20s and over 65s are less likely to hold a driving licence [14]. Data from the UK Electoral Commission reported that disadvantaged groups are more likely to not have an ID. For example, older people (aged 85+) were less likely to have an ID that was recognisable (91% compared to 95%–98% for those in younger age groups. It also found that the unemployed, people with disabilities, and people without qualifications, were all less likely to hold any form of photo ID [15].

Onboarding can be difficult for people who do not have access to technological resources or who are not technologically skilled. Not having an ID can have important implications for marginalised people as they may lack access to services that ensure credit accumulation or profit storage. As a consequence, marginalised people may have difficulty accessing many basic services, including work, social protection, banking or education. Likewise, the lack of a documented identity puts vulnerable and already marginalised people at constant risk of transgressing the lines between legal and illegal.

In recent years, digital identity verification through a mobile account has proven to be an effective verification method in several countries. This method has been used to prove identity in order to receive benefits from the government, private entities, or obtain microloans. Accessing financial services online or through mobile devices provides independence, the opportunity to pay daily expenses and to make longer-term plans, and therefore remove a key source of anxiety [16]. Having access to financial services helps marginalised groups not only to survive but also to bring themselves closer to the mainstream of society in terms of access whilst maintaining their individual identities, potentially facilitating a greater level of respect from those who do not find themselves marginalised. Poverty or social isolation driven by lack of access to services, including financial services, affects minorities in all nations.

In the western world, communities who are seen as being marginalised often correlate with low recorded levels of literacy, a lack of access to financial services and consequently a reliance on outside agencies, making this loosely confederated group a challenge to onboard to digital services [17]. Despite the fact that the richer countries, such as the United Kingdom, tend to have better quality services than poorer nations, the security that prevents unauthorised use of these services is much stricter. The cost of buying a passport or learning to drive to obtain a photo ID can easily prevent minorities from possessing these essential 'entrance' documents.

3 Digital Identity Onboarding

As noted above, a DI system is a mechanism that permits the creation and verification of an individual's identity using digital means. The process of using an identity within this system consists primarily of two steps: (i) onboarding, and (ii) authentication and ID management.

The implementation of these two phases incurs respective challenges. The onboarding phase contains many challenges that are social, economic, political and technological in nature. These include data collection, data verification, privacy, security, user experience, scalability and compliance.

The challenges faced during the authentication phase and ID management are analogous to those experienced in technological developments, for example: security, usability, scalability, false acceptance rate and false rejection rate, privacy, compliance and interoperability. Unlike the technological challenges in the authentication phase, which are dependent on the initial stage, the challenges in the onboarding phase are interdisciplinary in nature, making onboarding the referent object for a multidisciplinary inquiry, and requires a number of disciplinary perspectives and injects to generate solutions. As a result, it is crucial to formally address the challenges of the onboarding phase and design interdisciplinary solutions to create a trustable, efficient, and user-friendly experience.

The main obstacles in adopting DIs are: 1) the information gap that exists between the consuming public and the technology companies, and 2) people's hesitation to initially engage with the technology. Trust in technology in general, trust in a specific technology, and trust in the people and institutions behind a technology play an important role in shaping people's beliefs and behaviour [18, 19]. To establish trust, the DI system's onboarding, authentication, and ID lifecycle management processes must be demonstrated as trustworthy: this is both a measure that can be technically benchmarked and is also subject to sentiment. The consuming public's first impression and initial experience with a technology are also particularly important in shaping adoption and post-adoption behaviours [20]. Because these early beliefs and behaviours establish a path-dependency, we are identifying the DI onboarding phase as a key research consideration for ensuring equitable access and wide adoption of digital identities.

4 Achieving a Smooth Digital Identity Onboarding Experience

In order to increase the adoption of DIs, and to do so in a fair and equitable manner, we propose the use of physical locations for citizen onboarding to DI systems in the UK context. Such an approach has similarities to the use of Experience Centres (ECs) developed in other countries[1]. These ECs, which are physical locations, will allow users to register and collect digital IDs and credentials, and integrate them with other systems and services such as civil registration systems, e-sign, and elec-

tronic health records management.

An Experience Centre can facilitate trustworthy and inclusive onboarding to DI technologies. This has the potential both to address uneven access to DI technologies, and to increase DI adoption overall. Ensuring that access to DI technologies is inclusive can profoundly reduce inequalities as proving one's identity is rapidly becoming an essential part of exercising human rights on a day-to-day basis. The use of an EC is also to improve the efficiency of the DI onboarding process with additional services taking place on-site, such as document verification, biometric capture, and identity document scanning. Such an EC would provide a secure and user-friendly environment for users to interact with the DI system, close the information gap between the public and DI providers, and develop confidence in the technology and related services. ECs also allow us to iterate and improve the user experience within them, thus constantly improving accessibility and trust. We envision an EC as a *Digital Identity Playground* that can positively shape citizens' first impression with the technology and, in turn, promote adoption of DI technologies.

ECs are complex sociotechnical systems and, as such, are very difficult to design and implement [21]. A number of considerations need to be taken into account in order to address fundamental design questions, such as:

- What are the most important features and services of a model EC in the UK?

- What are the specific requirements of a model EC in terms of technical infrastructure, staffing, spatial architecture, cost and security?

- What are the main design considerations to ensure that the model EC can engage citizens in an inclusive manner, increase adoption, build confidence in the use of DIs, and act effectively as a digital playground?

5 Our Research Approach

To operationalise our *multidisciplinary* approach we have designed a series of research activities and methods that are necessary steps to effectively address these questions. The contribution from Foreign Policy Analysis (FPA) of *Horizon scanning* will be used to identify the key drivers shaping the DI onboarding operational environment and key action points to proactively shape desirable futures. The output of a horizon scan is a formal assessment document that provides a probabilistic measure of likelihood of various future trends occurring and allows the recipient to make evidence based judgements about resourcing and framing responses to the initial challenge. In this context, the horizon scan will identify trends over the ten-year time period, from most likely to wild card possibilities, and also provide assessments of the sourcing base for these judgements. The output from the horizon scan will exist as a standalone document, but also helps to inform the creation of requirements (e.g., specific use cases and design

---

[1]https://mosip.io/news-events/announcing-the-launch-of-the-first-mosip-experience-centre-an-end-to-end-walk-in-mosip-experience-in-bangalore-india

diagrams) and recommendations, that in turn provide an underpinning for the design of an Experience Centre. In general terms, a horizon scan is an empiricist tool for identifying the key elements of the phenomena or issue in hand - in this case onboarding. Further, a horizon scan assists in generating areas for further research, action and mitigation [22].

The contribution from Operational Sciences and Human-Computer Interaction is a *Literature review and science mapping analysis* which aims at investigating the state of the current research and also the implementation trends and opportunities in DIs with a specific focus on the onboarding process. This structured analysis of this large body of academic information relating to DIs will allow us to infer research trends over time, recognise themes, identify shifts in the boundaries of the disciplines, detect the most prolific scholars, institutions and countries, and to present the 'big picture' of extant research around DI systems, user adoption and onboarding [23, 24].

Semi-structured interviews - derived from a social scientific underpinning - will help to provide an understanding of stakeholder and end-user perceptions and attitudes towards DI systems, with a focus on inclusivity as a framing device within onboarding. The main purpose of the interviews with stakeholders will be to investigate possible challenges, barriers, attitudes and opportunities and identify major trends to inform the development and design of future trustworthy digital identities that guarantee equality and inclusion and are accessible for all. Moreover, by interviewing stakeholders we will be able to understand how ECs can ensure an equal and inclusive society.

Finally, *Threat and risk assessment* will determine the methods, practices, and approaches that provide the greatest traction for identifying and assessing security threats and evaluating the associated risks for inclusivity in future digital identity onboarding systems. A threat and risk assessment encompasses a comprehensive examination of both the users and the digital identity system for potential threats and the subsequent evaluation of the associated security risks. This assessment takes into account the likelihood and potential impact of a threat event occurring, as well as the capability of a threat actor to exploit any weaknesses within the system. Based on the level of threat and risk identified, appropriate risk management strategies can be developed, which may include the acceptance of the risk, the implementation of mitigation measures, or the adoption of avoidance strategies [25, 26].

We expect that this combination of policy perspective, multidisciplinary academic perspectives, the perspective of end-users and stakeholders, and the technical and security perspectives will complement one another to provide a more complete picture of what is required for the development of an EC in a UK context. This, in turn, can be very useful input for policy making, regulation and inform best practices and specifications for the DIATF.

Two types of results are expected from these research activities. First, this research approach will provide a set of requirements and specifications that can be used for the design and operation of a model EC. These will take the form of commonly used artefacts that are used for this purpose, such as use case descriptions, use case diagrams, data flow diagrams and process flow diagrams. These will not be meant to provide an exhaustive set of rigid specifications, but instead will focus on the DI-specific characteristics of the design and operation of an EC. The focus will also be on addressing 'pain points' or 'critical incidents' [27] identified in the onboarding process. These artefacts also have the potential to be used as 'boundary objects' to facilitate communication, engagement and feedback from stakeholders [28, 29]. Second, we expect to provide a set of qualitative recommendations that arise from these research activities. These recommendations will ensure that aspects of citizen inclusion and empowerment are adequately addressed (e.g., taking into account the needs of diverse groups of citizens), and will provide more flexibility in the output.

6 Conclusion

The implementation of a social inclusive and technically robust onboarding process for digital identities is a under-emphasised but highly impactful component of the development of digital identifies. It is an important element of the future economic success of the UK, the trust and participation of all elements of the British society in this digital future, and the strength of digitally plaformed or cyber-influenced social relationships within the UK and outside. The multidisciplinary research approach outlined in this work will provide impact-laden research that can be utilised by government policy officials and technology partners to improve their DI offers.

Acknowledgements

References

[1] K.-L. Tan, C.-H. Chi, and K.-Y. Lam, "Analysis of digital sovereignty and identity: From digitization to digitalization," 2022. [Online]. Available: https://arxiv.org/abs/2202.10069

[2] UK Government, "Uk digital identity and attributes trust framework beta version (0.3)," 2023. [Online]. Available: https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version/uk-digital-identity-and-attributes-trust-framework-beta-version

[3] T. Spiliotopoulos, D. Horsfall, M. Ng, K. Coopamootoo, A. van Moorsel, and K. Elliott, "Identifying and supporting financially vulnerable consumers in a privacy-preserving manner: A use case using decentralised identifiers and verifiable credentials," in *Designing for New Forms of Vulnerability workshop at CHI 2021*, 2021.

[4] F. Wang and P. De Filippi, "Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion," *Frontiers in Blockchain*, vol. 2, pp. 1–22, 2020.

[5] K. Elliott, K. Coopamootoo, E. Curran, P. Ezhilchelvan, S. Finnigan, D. Horsfall, Z. Ma, M. Ng, T. Spiliotopoulos, H. Wu, and A. van Moorsel, "Know your customer: Balancing innovation and regulation for financial inclusion," *Data & Policy*, vol. 4, 2022.

[6] A. Beduschi, "Rethinking digital identity for post-covid-19 societies: Data privacy and human rights considerations," *Data & Policy*, vol. 3, 2021.

[7] L. Ante, C. Fischer, and E. Strehle, "A bibliometric review of research on digital identity: Research streams, influential works and future research paths," *Journal of Manufacturing Systems*, vol. 62, pp. 523–538, 2022.

[8] K. Kameron, "The laws of identity," 2005. [Online]. Available: http://myinstantid.com/laws.pdf

[9] European Commission, "Commission proposes a trusted and secure digital identity for all europeans," 2021. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663

[10] ——, "eidas regulation," 2022. [Online]. Available: https://digitalstrategy.ec.europa.eu/en/policies/eidas-regulation

[11] S. Masiero and V. Arvidsson, "Degenerative outcomes of digital identity platforms for development," *Information Systems Journal*, vol. 31, no. 6, pp. 903–928, 2021.

[12] A. Martin and L. Taylor, "Exclusion and inclusion in identification: regulation, displacement and data justice," *Information Technology for Development*, vol. 27, no. 1, pp. 50–66, 2021.

[13] D. Z. Davis and K. Chansiri, "Digital identities – overcoming visual bias through virtual embodiment," *Information, Communication & Society*, vol. 22, no. 4, pp. 491–505, 2019.

[14] The Electoral Commission, "2019 report: Accuracy and completeness of the 2018 electoral registers in great britain," 2019. [Online]. Available: https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/our-views-and-research/our-research/accuracy-and-completeness-electoral-registers/2019-report-accuracy-and-completeness-2018-electoral-registers-great-britain

[15] Electoral Reform Society, "Briefing on mandatory voter id at the polling station," 2021. [Online]. Available: https://www.electoral-reform.org.uk/latest-news-and-research/parliamentary-briefings/briefing-on-mandatory-voter-id-at-the-polling-station/

[16] E. C. Brüggen, J. Hogreve, M. Holmlund, S. Kabadayi, and M. Löfgren, "Financial well-being: A conceptualization and research agenda," *Journal of Business Research*, vol. 79, pp. 228–237, 2017.

[17] P. K. Ozili, "Financial inclusion research around the world: A review," *Forum for Social Economics*, vol. 50, no. 4, pp. 457–479, 2021.

[18] D. H. McKnight, M. Carter, J. B. Thatcher, and P. F. Clay, "Trust in a specific technology: An investigation of its components and measures," *ACM Transactions on Management Information Systems*, vol. 2, no. 2, pp. 1–25, 2011.

[19] T. Guggenberger, L. Neubauer, J. Stramm, F. Volter, and T. Zwede, "Accept me as i am or see me go: A qualitative analysis of user acceptance of self-sovereign identity applications," in *HICSS 2023*, 2023.

[20] G. Fox, T. Clohessy, L. van der Werff, P. Rosati, and T. Lynn, "Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications," *Computers in Human Behavior*, vol. 121, p. 106806, 2021.

[21] G. Baxter and I. Sommerville, "Socio-technical systems: From design methods to systems engineering," *Interacting with Computers*, vol. 23, no. 1, pp. 4–17, 2011.

[22] P. Hines, L. Hiu Yu, R. Guy, A. Brand, and M. Papaluca-Amati, "Scanning the horizon: a systematic literature review of methodologies." *BMJ Open*, vol. 9, no. 5, p. e026764, 2019.

[23] C. Chen, "Science mapping: A systematic review of the literature," *Journal of Data and Information Science*, vol. 2, no. 2, pp. 1–40, 2017.

[24] M. Aria and C. Cuccurullo, "bibliometrix: An r-tool for comprehensive science mapping analysis," *Journal of Informetrics*, vol. 11, no. 4, pp. 959–975, 2017.

[25] A. Shostack, *Threat Modeling: Designing for Security*. John Wiley & Sons, 2014.

[26] T. Sheik, C. Maple, and G. Epiphaniou, "Considerations for secure mosip deployment," in *Competitive Advantage in the Digital Economy (CADE 2022)*. Institution of Engineering and Technology, 2022.

[27] L. D. Butterfield, W. A. Borgen, N. E. Amundson, and A.-S. T. Maglio, "Fifty years of the critical incident technique: 1954-2004 and beyond," *Qualitative Research*, vol. 5, no. 4, pp. 475–497, 2005.

[28] C. P. Lee, "Boundary negotiating artifacts: Unbinding the routine of boundary objects and embracing chaos in collaborative work," *Computer Supported Cooperative Work (CSCW)*, vol. 16, no. 3, pp. 307–339, 2007.

[29] J. Vines, R. Clarke, P. Wright, J. McCarthy, and P. Olivier, "Configuring participation: On how we involve people in design," in *SIGCHI Conference on Human Factors in Computing Systems - CHI '13*. New York, New York, USA: ACM Press, 2013, p. 429.