KHAZANAH RESEARCH INSTITUTE

VIEWS 3/26 | 26 February 2026

The Iceberg of Everyday Digital Identity

Salbiah Idris

Views are short opinion pieces by the author(s) to encourage the exchange of ideas on current issues. They may not necessarily represent the official views of KRI. All errors remain the author's own.

This view was prepared by Salbiah Idris, a researcher from the Khazanah Research Institute (KRI). The author is grateful for the valuable comments from Dr Rachel Gong.

Author's email address:
salbiah.idris@krinstitute.org

Information on Khazanah Research Institution publications and digital products can be found at www.KRInstitute.org.

Introduction

This Views builds on the analytical foundations set out in *Assessing and Optimising MyDigital ID*[1], a recent discussion paper that assessed digital identity through system-level considerations such as legal authority, institutional governance, inclusion and readiness to scale using MyDigital ID as an illustrative case. That analysis focused primarily on design, governance and comparative experience. This Views shifts the lens from how digital identity systems are built to how they are encountered in everyday use, paying particular attention to moments of friction, failure and disengagement that tend to fall outside system-level assessments but are central to trust, legitimacy and long-term sustainability.

Digital identity is often presented as a practical enhancement to public administration. By replacing paper-based credentials with secure digital verification, governments can deliver services more quickly, at lower cost and with greater

[1] Salbiah Idris (2026)

consistency. For example[2], Estonia's X-Tee data-sharing platform saves the government and residents over 820 years of collective work annually. In Singapore, electronic know-your-customer (eKYC) processes facilitated by Singpass consented data sharing have reduced digital transaction times by approximately 80%. Meanwhile, in India, the Aadhaar system has decreased eKYC onboarding costs from about USD 23 to less than USD 0.15 each person. Digital identity has also been associated with fraud reduction[3]. In India, linking digital ID to public sector wage and benefit payments has helped plug payment leakages, contributing to an estimated 13.4% improvement in household incomes. These efficiency and integrity gains help explain why digital identity continues to attract strong political and institutional support.

Yet digital identity is not only a tool for efficiency. In practice, it functions as an access system that increasingly shapes how people interact with government, the private sector and essential services. When it works smoothly, it fades into the background of everyday life. When it falters, even briefly, it can disrupt access to income, government assistance, healthcare, education or employment. These disruptions are not experienced evenly and have uneven effects on users. While some users recover quickly with minimal effort, others face repeated barriers, disengage quietly or are excluded altogether.

The iceberg metaphor helps to make this imbalance visible. Above the surface sit the benefits that are easy to observe, measure and celebrate, such as speed, scale and convenience. Below the surface lie less visible experiences of friction, failure, uneven recovery and silent withdrawal. These everyday dynamics shape whether digital identity systems remain trusted and usable over time. Paying attention to what lies beneath the surface is essential because its long-term stability depends on how well it functions under imperfect conditions.

Above the Surface

Why Digital Identity Works

Digital identity systems persist and expand because they deliver efficiency, scale and consistency in ways that are tangible for both users and governments.

For individuals, the most immediate benefit is time saved. Digital identity reduces the need for repeated manual checks and physical visits by enabling remote verification. Evidence shows substantial reductions in transaction times for routine activities such as opening bank accounts, applying for permits or registering businesses[4]. These gains matter because they reduce travel costs, minimise time away from work and lower the likelihood of clerical error. Convenience in this context is meaningful because it directly determines whether people can realistically access services.

[2] World Bank (2025)
[3] UNDP (2023)
[4] World Bank (2023); WEF (2021)

For governments, the advantages grow with scale. Digital identity enables standardised verification, automated compliance and the consolidation of records across agencies[5]. This can significantly reduce onboarding costs in regulated sectors and improve welfare integrity by limiting fraud and duplication[6]. Once these efficiencies are realised, digital identity becomes embedded as core infrastructure rather than an optional service. Its value increases further when identity can be reused across sectors, reducing duplication for both institutions and users[7].

These operational benefits also explain political support. Digital identity performs well during crises by enabling remote service delivery when physical offices are closed[8]. It supports fiscal discipline[9] and is often framed as a foundation for economic growth and digital transformation. Where systems are accompanied by clear governance and safeguards, they can attract broad public backing. At the surface, digital identity appears efficient, fair and future-ready.

Why Digital ID Is Appealing

Public narratives around digital identity are shaped by outcomes that are easy to observe and quantify. For users, the most visible benefit is reduced inconvenience. For policymakers, it is cost savings, fraud reduction and high coverage. These outcomes translate neatly into performance indicators[10], making them powerful signals of success.

Standardisation reinforces these narratives. Automated identity checks and defined assurance levels create the impression that everyone is subject to the same rules[11]. Compared with discretionary, face-to-face verification, digital processes can appear more objective and less prone to error or corruption[12]. Consistency is therefore often experienced as fairness.

However, the appearance of consistency does not guarantee a consistent experience for all users. Even when enrolment is high and the system generally works as intended, some users continue to face repeated difficulties[13]. These experiences are easy to miss because they sit outside overall measures of how the system performs[14]. In some contexts, high uptake reflects necessity rather than trust, with registration becoming effectively mandatory to access basic services[15]. When success is defined primarily by speed and coverage, the lived experience of those who fall outside the smooth path is easily overlooked.

This is where the iceberg metaphor becomes useful. The visible tip reflects what systems do well under ideal conditions. Below the surface lie the conditions under which systems pause, fail or demand extra effort from users, revealing how resilient and inclusive they really are.

[5] World Bank (2025); OECD (2024); UNCDF (2022); WEF (2021)
[6] Ibid.
[7] WEF (2021)
[8] OECD (2021)
[9] World Bank (2016)
[10] World Bank (2018)
[11] OECD (2023); World Bank (2019)
[12] World Bank (2019); Clark and Daly (2019)
[13] World Bank (2019)
[14] WEF (2018)
[15] Anand and Brass (2021); World Bank (2019)

Below the Surface

Everyday friction and uneven recovery

Digital identity systems function as access gates. When the gate fails, access to everything behind it is interrupted. Even short-lived disruptions can therefore have significant and lasting consequences.

Failures arise in many ways. Remote authentication can break down due to network instability[16] and activation processes may fail under high demand[17]. Enrolment requirements, particularly those involving in-person biometric capture, can become bottlenecks when service points are distant or difficult to reach[18]. Each disruption interrupts what users expect to be a seamless interaction. These interruptions generate more than inconvenience. Repeated friction can produce frustration and erode confidence. When access is blocked, people look for workarounds. They may share credentials, reuse passwords or rely on unofficial intermediaries[19]. In this way, systems meant to improve security can unintentionally undermine it.

Crucially, system failures do not affect all users equally[20]. The ability to recover from disruption depends heavily on socio-economic position, physical ability and access to support. Poor and rural residents may lack reliable connectivity or the resources to travel to service points[21]. Persons with disabilities may face inaccessible interfaces or support channels[22]. Displaced people often lack the necessary documents to reestablish their identity after a disruption[23]. Women may face additional barriers when ownership gaps or mobility constraints limit their ability to engage in independent problem-solving[24]. Manual workers and older adults are more likely to experience biometric mismatch as physical labour and ageing alter fingerprints or facial features[25].

Recovery is therefore not only technical. It depends on digital skills, confidence and social networks. Individuals with higher digital literacy and stronger support systems tend to recover more easily[26]. Marginalised users are more likely to accept rejection as final because they have limited ability to negotiate within strict electronic systems frameworks[27]. Over time, small recurring failures accumulate, leading to insecure coping strategies that cause people to revert to paper-based options and erode trust in public institutions.

[16] Anand and Brass (2021)
[17] Halliday (2025)
[18] Anand and Brass (2021); Beduschi (2021)
[19] Gallistl et al. (2021)
[20] Gallistl et al. (2021); Kuntsman and Miyake (2022)
[21] Anand and Brass (2021)
[22] Kuntsman and Miyake (2022)
[23] Beduschi (2021)
[24] Anand and Brass (2021)
[25] Ibid.
[26] Gallistl et al. (2021)
[27] Karren, Schmitz, and Schaffer (2024)

Invisibility, silence and governance blind spots

As digital identity systems mature, verification increasingly happens in the background[28]. Automation improves convenience but reduces visibility and understanding.

When processes become invisible, users find it hard to develop accurate mental models of how decisions are made or how their data is shared[29]. Some respond with indifference, assuming the system is too complex to understand or adopting the principle that they should not need to understand how a service works to use it[30]. Others overestimate its sophistication[31]. Trust built on misunderstanding is fragile and can collapse when unexpected errors occur. When automated systems fail, the lack of transparency can hinder the ability to understand and make sense of the situation[32]. Users cannot easily determine whether the problem lies with their device, the network, the data or the decision logic itself[33]. This uncertainty fuels frustration and risky behaviour, including the sharing of sensitive documents through insecure channels[34].

At the same time, many access problems are never reported[35]. Instead of complaining, users disengage. People are most likely to withdraw silently when onboarding is complex, when account creation is forced, when feedback is poor or when seeking help feels frustrating[36]. Silent disengagement is more common among individuals with low digital literacy, limited connectivity, high levels of distrust or heavy documentary requirements[37]. Internalised blame plays a powerful role[38]. When failure is interpreted as a personal shortcoming rather than a system flaw, users are less likely to seek redress and more likely to withdraw permanently[39].

For policymakers, this silence creates a governance blind spot. Systems can appear successful based on adoption rates and helpdesk data while excluding substantial numbers of people. Without mechanisms to identify friction, non-use and informal workarounds, harms stay hidden and corrective actions are delayed.[40].

[28] Ferraz and Ferraz (2021)
[29] Springer and Whittaker (2020)
[30] Ibid.
[31] Ibid.
[32] Ibid.
[33] Kuntsman and Miyake (2022)
[34] Ferraz and Ferraz (2021); Kuntsman and Miyake (2022)
[35] Karren, Schmitz, and Schaffer (2024)
[36] Karren, Schmitz, and Schaffer (2024); Kuntsman and Miyake (2022); Ferraz and Ferraz (2021)
[37] Kuntsman and Miyake (2022); Gallistl et al. (2021); Anand and Brass (2021)
[38] Gallistl et al. (2021)
[39] Karren, Schmitz, and Schaffer (2024); Gallistl et al. (2021)
[40] Carrillo et al. (2023); Anand and Brass (2021); Gallistl et al. (2021)

Conclusion

Digital identity has established itself as a core component of modern public infrastructure. It delivers real benefits by saving time, reducing costs, limiting fraud and bringing consistency to service delivery. These gains are significant and should not be discounted.

Long-term stability relies on managing both what is visible on the surface and what lies beneath it. Every day, friction contributes to the formation of exclusion. Temporary breakdowns are moments when trust is put to the test. Automation, when lacking transparency, undermines personal autonomy. Additionally, silence may indicate withdrawal rather than satisfaction.

The iceberg metaphor serves not only as a description but also as a policy guide. Digital identity systems that concentrate solely on visible successes risk becoming fragile and unfair. In contrast, systems that consistently focus on hidden experiences, especially how individuals recover from failures, might be more likely to be resilient, inclusive and deserving of public trust.

References

Anand, Nishant, and Irina Brass. 2021. "Responsible Innovation for Digital Identity Systems." *Data & Policy* 3 (January):e35. https://doi.org/10.1017/dap.2021.35.

Beduschi, Ana. 2021. "Rethinking Digital Identity for Post-COVID-19 Societies: Data Privacy and Human Rights Considerations." *Data & Policy* 3 (January):e15. https://doi.org/10.1017/dap.2021.15.

Carrillo, Eduardo, Catalina Frigerio, María Jesús Valenzuela, Alessia Aquaro, Jean-Christophe Mauduit, Ine Steenmans, and María Paz Sandoval. 2023. "The Performance Gap of Policy Information Systems: A Knowledge Infrastructure Assessment Framework." *Journal of Science Policy & Governance* 22 (1). https://doi.org/10.38126/JSPG220105.

Clark, Julia Michal, and Conrad Charles Daly. 2019. "Digital ID and the Data Protection Challenge : Practitioner's Note." Working Paper 142702. World Bank Group. https://documents1.worldbank.org/curated/en/508291571358375350/pdf/Digital-ID-and-the-Data-Protection-Challenge-Practitioners-Note.pdf.

Ferraz, André, and Carlos Ferraz. 2021. "Digital Identity Challenge: The Security and Convenience Dilemma." In *Integrated Software and Hardware Seminar (SEMISH)*, 251–56. SBC. https://doi.org/10.5753/semish.2021.15829.

Gallistl, Vera, Rebekka Rohner, Lisa Hengl, and Franz Kolland. 2021. "Doing Digital Exclusion – Technology Practices of Older Internet Non-Users." *Journal of Aging Studies* 59 (December):100973. https://doi.org/10.1016/j.jaging.2021.100973.

Halliday, Nnennaya. 2025. "A Conceptual Framework for Financial Network Resilience Integrating Cybersecurity, Risk Management, and Digital Infrastructure Stability." *International Journal of Advanced Multidisciplinary Research and Studies* 3 (2):1253–63.

Karren, Kai, Michael Schmitz, and Stefan Schaffer. 2024. "Improving Conversational User Interfaces for Citizen Complaint Management through Enhanced Contextual Feedback." In *Proceedings of the 6th ACM Conference on Conversational User Interfaces*, 1–11. CUI '24. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3640794.3665562.

Kuntsman, Adi, and Esperanza Miyake. 2022. *Paradoxes of Digital Disengagement: In Search of the Opt-Out Button*. University of Westminster Press. https://doi.org/10.16997/book61.

OECD. 2021. "G20 Collection of Digital Identity Practices: Report for the G20 Digital Economy Task Force." Trieste, Italy: Organisation for Economic Co-operation and Development (OECD).

———. 2023. "Recommendation of the Council on the Governance of Digital Identity." OECD. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491.

———. 2024. "Digital Public Infrastructure for Digital Governments, OECD Public Governance Policy Papers." 68.

Salbiah Idris. 2026. “Assessing and Optimising MyDigital ID.” Kuala Lumpur: Khazanah Research Institute. https://www.krinstitute.org/publications/assessing-and-optimising-mydigital-id-3.

Springer, Aaron, and Steve Whittaker. 2020. “Progressive Disclosure: When, Why, and How Do Users Want Algorithmic Transparency Information?” *ACM Trans. Interact. Intell. Syst.* 10 (4):29:1-29:32. https://doi.org/10.1145/3374218.

UNCDF. 2022. “The Role Of Electronic Transactions And National Digital Id Systems In The Digital Economy.” UNCDF / Policy Accelerator (United Nations Capital Development Fund). https://static1.squarespace.com/static/5f2d7a54b7f75718fa4d2eef/t/621d4545d668f30b5c35eab3/1646085472035/EN-UNCDF-Brief-ElectronicID-2022.pdf.

UNDP. 2023. “Accelerating the SDGs through Digital Public Infrastructure.” UNDP (United Nations Development Programme). https://www.undp.org/sites/g/files/zskgke326/files/2023-08/undp-g20-accelerating-the_sdgs-through-digital-public-infrastructure.pdf.

WEF. 2018. “Identity In A Digital World: A New Chapter In The Social Contract.” World Economic Forum. https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf.

———. 2021. “Digital Identity Ecosystems: Unlocking New Value.” https://www3.weforum.org/docs/WEF_Guide_Digital_Identity_Ecosystems_2021.pdf.

World Bank. 2016. “Digital Identity : Towards Shared Principles For Public And Private Sector Cooperation.” Working Paper 107201. World Bank Group. https://documents1.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf.

———. 2018. “Technology Landscape for Digital Identification.” Washington DC: The World Bank. https://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf.

———. 2019. “ID4D Practitioner’ Guide: Version 1.0.” Version 1.0. Washington DC, United States: The World Bank. https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf.

———. 2023. “Putting People at the Center of Digital Public Infrastructure (DPI): Annual Report 2023.” Text/HTML. World Bank Group. 2023. https://documents1.worldbank.org/curated/en/099647503042425828/pdf/IDU-a9d1a6be-30dc-48e6-9318-cf9d26959fb9.pdf.

———. 2025. “Digital Public Infrastructure and Development: A World Bank Group Approach. Digital Transformation White Paper, Volume 1.” Volume 1. Washington DC, United States: The World Bank. https://documents1.worldbank.org/curated/en/099031025172027713/pdf/P505739-84c5073b-9d40-4b83-a211-98b2263e87dd.pdf.