JULY 2024

YIANNIS THEODOROU
CAMPBELL COWIE
RYLEY CHARLWOOD

Creating Value for Users and Governments: How AI Can Enhance Digital-ID Solutions

TONY BLAIR
INSTITUTE FOR
GLOBAL CHANGE

The commentary is co-authored in partnership with iProov.

The global shift towards digital public services has accelerated rapidly, driven by technological progress, higher consumer expectations around online experiences created by private-sector innovation and the catalytic effect of the pandemic. For developing nations, digitalisation and digital inclusion are crucial for socioeconomic growth. For industrialised economies, they are key to meeting citizens' evolving needs and achieving new priorities, such as net zero.

Governments' efforts to transform public-service delivery using digital technologies have now indisputably gained momentum. For many countries, a secure and trustworthy digital-identity system serves as the foundation for this change. Digital ID is the digital representation of your identity. It enables automated access to online services, remote identity verification and management of digital interactions, serving as a virtual equivalent of physical identification. It transforms how governments and citizens interact, expands participation through inclusion and can enable seamless access to public and private-sector services.

Recent advances in the use of artificial intelligence put governments at a unique technological inflection point; one with immense potential to catalyse digital transformation and propel economic growth. However, the presence of malicious actors using AI to attack public services for financial and other rewards creates a multi-faceted challenge: how can governments accelerate the digital economy, drive economic participation through inclusion and enhance service delivery *without* compromising citizens' privacy or data protection?

International cooperation and proactive, informed policymaking are essential during this period. Now is the time to determine how best to shape the future to reap its rewards.

This commentary explores practical, everyday applications of AI-powered digital-ID solutions that create tangible value and convenience for users and governments.

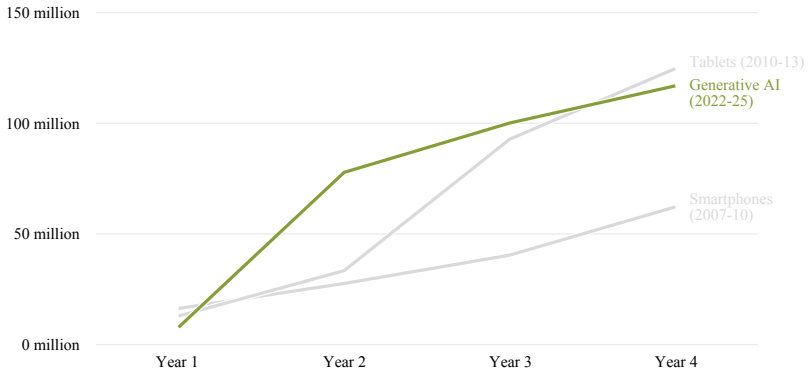
AI's Role in Enhancing Digital ID

The economic importance of digital-ID systems is clear; they promote socioeconomic growth through participation, modernisation, innovation, personalisation and efficiency in public services.

It is no secret that the proliferation of connectivity and smartphones, corresponding improvements in user experience across digital channels, and conducive governmental policies have fuelled economic growth over the past two decades. However, generative AI – and its rapid adoption over the past two years, outpacing all recent technologies – has introduced a truly novel dimension to digital transformation.

FIGURE 1

Generative AI has a steeper initial adoption curve than other recent technologies (units: millions of US users)



Source: Insider Intelligence June 2023

Note: Individuals of any age who use each technology at least once per month; Year 1 for smartphones corresponds with the June 2007 release of the iPhone; Year 1 for tablets corresponds with the April 2010 release of the iPad; Year 1 for generative AI corresponds with the November 2022 release of ChatGPT.

Just as computers drastically enhanced government capabilities, AI enables data analytics and informed decision-making at an unprecedented and personalised scale, boosting productivity and transforming service delivery.

Where verifying a user's identity (or identity-linked credentials) is important in the context of an AI-powered service, digital ID can enhance the quality of data fed into AI systems, ensuring more reliable and accurate AI outputs across all contexts. By mitigating the risk of "garbage in, garbage out", digital ID acts as an enabler of more trusted and reliable data.

AI can support and augment digital-ID outcomes in several key areas:

- **Enhanced user experience, support and accessibility**: AI chatbots and virtual assistants can provide real-time support for citizens using digital-ID systems. For example, the mAigov tool, an AI-driven chatbot launched by Greece's Ministry of Digital Governance, is embedded within the country's digital-government portal (gov.gr). It enables citizens to access 1,832 digital public services seamlessly and receive personalised responses to their questions.
- **Personalised and targeted services**: By analysing data linked to digital ID, AI can enable governments to deliver more targeted social services, health-care interventions and educational resources. For instance, Singapore is working to integrate AI for disease diagnosis, patient monitoring and predictive health-care analytics. In the education sector, AI-powered digital tutors such as OpenAI's GPT-4o analyse students' progress and needs, providing personalised and adaptive materials, explanations and support. Virtual, personalised learning can truly revolutionise education globally.
- **Data-informed decision-making**: AI, when trained on trusted data, can analyse new information and identify patterns, enabling smarter decision-making. In health-care, AI can flag scans requiring specialist attention, reducing unnecessary diagnostic tests. It can also enhance pharmaceutical trials, though this requires robust security measures for accessing patients' data and managing consent. The NHS App, used by the UK's National Health Service, exemplifies how access to health data and appointment booking can be securely managed, with over 30 million sign-ups. Looking ahead, integrating health and medication information into digital wallets with selective disclosure features could give patients greater control over their records, further revolutionising access to and management of health-care data.
- **Automated identity verification and fraud detection (the war against fraudsters)**: AI algorithms can automate the identity-verification process, detect fraudulent activities through pattern recognition and enhance security. For example, the UK Home Office uses biometric technology to automate applications to the EU Settlement Scheme, allowing secure remote identity verification without any in-person appointments. Governments in particular require the highest levels of security afforded

by AI. The European Union Agency for Cybersecurity's (ENISA) Threat Landscape 2023 report identified public administration as the "most targeted sector", drawing 19 per cent of targeted cyber-attacks.

Digital-ID Success Spotlights

Certain countries are at the forefront of digital transformation, leveraging AI and digital ID to create tangible impacts:

- **Singapore's** digital-identity solution, Singpass, provides citizens with secure access to online services and facilitates more than 500 million personal and corporate transactions each year. Onboarding and authentication are secured by biometric technology, utilising AI and machine learning to identify genuine account owners; for example through liveness-detection capabilities. Available services include applying for financial-support schemes, renewing licences and accessing health records without requiring in-person interactions.
- **Estonia's** Smart-ID allows citizens worldwide to authenticate their identities, access e-services and provide digital signatures online (recognised as equivalent to handwritten signatures under the EU's eIDAS regulation, which sets out a framework for digital identity and authentication) from anywhere. The Smart-ID mobile app uses AI and machine-learning-powered technologies such as near-field communication-based document-verification technology and facial-verification technology to establish trust in user identity and deter fraud.
- **Finland's** Finnish Trust Network (FTN) consolidates various electronic identification methods, including bank ID and mobile ID, to provide secure online authentication for millions of transactions annually. While the core framework utilises traditional eID methods, third-party providers enhance security with AI-powered solutions such as document verification and biometric analysis. FTN enables citizens to access government services, conduct financial transactions and perform other critical online activities without in-person interactions. This comprehensive approach ensures strong authentication and compliance with EU standards, significantly streamlining digital-identity verification processes across Finland.

TBI analysis shows that the UK could implement a digital-ID system within three years and generate cumulative net savings of almost £4 billion during this Parliament and nearly £10 billion during the next term.

Mitigating AI-Related Risks in Digital-ID Systems

Despite the benefits, integrating AI into digital-ID systems is not without risks. A significant concern is the potential for synthetic media – video, images, text or voices generated by AI – to create convincing but fake digital identities, enabling identity theft, fraud and challenging election integrity.

The rise of generative AI has made creating realistic synthetic media alarmingly easy. As the Alan Turing Institute articulates, it's now "increasingly challenging, potentially even impossible, to reliably discern between authentic and synthetic media". ENISA's recent report on digital-ID best practices also questions the sustainability of solutions relying upon even the most expert human examiners.

Human inspection is therefore not a viable solution. Biometric liveness-detection solutions, which often use AI to detect AI, have become crucial in ensuring authenticity.

AI-driven threats are rapidly evolving, with biometric vendors such as iProov regularly publishing data on emerging sophisticated AI-driven attacks. iProov's latest report uncovered a staggering 704 per cent increase globally in "sophisticated face swap attacks" in 2023 alone, highlighting the scale of this problem.

Leveraging AI responsibly, governments can enhance digital-ID security and adapt to threats:

- **AI-driven deepfake detection**: Machine-learning models trained to recognise the subtle inconsistencies in synthetic media can help identify and flag potential deepfakes, ensuring the authenticity of digital ID when used online.

- **Enhanced cyber-security measures**: AI can strengthen cyber-security protocols by continuously monitoring digital-ID systems for unusual activity and potential breaches, swiftly identifying and counteracting malicious attempts to manipulate digital-ID transactions. The US Department of Homeland Security is leveraging AI and machine learning to enhance its capabilities; its EINSTEIN system monitors federal networks, analysing terabytes of data each day with advanced network-anomaly alerting.
- **Continuous learning and adaptation**: AI systems can learn and adapt continuously, improving their ability to detect and respond to new threats over time, which is crucial in staying ahead of bad actors whose tactics are constantly evolving. A security-operations centre and cloud-based deployment usually achieves this, enabling 24/7 real-time monitoring and rapid security updates.

Proactively leveraging AI, governments can build secure, trusted digital-ID ecosystems enabling transformative technology adoption.

The Role of Regulations and Standards

Robust regulatory frameworks and standards are critical for ensuring the responsible adoption of digital-ID systems and AI technologies. A significant development in the digital-ID landscape is the recent adoption of the eIDAS 2.0 regulation in Europe. This updated regulation sets a new standard for digital identities, emphasising security, interoperability, user control and respect for privacy.

With eIDAS 2.0, the European Commission aims to create a seamless digital-ID ecosystem across EU member states, making digital identities equivalent to face-to-face identification and handwritten signatures across the continent. This regulation will likely set the bar for other countries, influencing global standards for digital-ID systems. eIDAS encourages secure cross-border transactions, including access to government services, and provides a model for doing so.

In addition to eIDAS 2.0, the EU's Artificial Intelligence Act seeks to regulate AI technologies by setting high standards for safety, transparency and accountability. Support is also provided by related rules on cyber-security and consumer protection. As more nations pursue secure digital-ID systems and responsible use of AI, these EU frameworks will provide guidance, enabling innovation while influencing governance globally.

The World Bank's ID4D initiative highlights the need for a balanced approach to digital-ID systems that promotes innovation while implementing necessary safeguards. ID4D sets out clear recommendations for governments to invest in R&D, robust regulations, public awareness, strong security protocols and international collaboration with stakeholders across sectors. Following such a comprehensive strategy can enable the responsible development of digital-ID systems that harness AI's benefits while mitigating associated risks.

Recommendations for Governments

To harness the opportunities and mitigate the risks associated with AI in digital-ID contexts, governments should consider the following recommendations:

- **Invest in AI research and development**: Create robust systems capable of enhancing digital-ID security and functionality. Collaboration with academia and the private sector can accelerate innovation. The US Department of Homeland Security provides a positive example, with a clear road map emphasising responsible AI adoption through strategic partnerships, academic collaboration and a commitment to safeguarding privacy.
- **Implement comprehensive frameworks**: Balance digital-ID innovation with guardrails on privacy, security and ethical AI. Leadership should focus on demand-driven use cases and positive user experiences. Frameworks should require that providers deliver inclusion, accessibility and security to unlock digital-transformation benefits and build public trust.

- **Promote public awareness and education**: Inform citizens about data sharing and privacy protections. Offer privacy-preserving solutions that give citizens more control over their personal data. Combine awareness with technological interventions. Be careful not to place the burden on citizens, though: people can no longer reliably spot deepfakes, for example, so we cannot "educate" problems surrounding synthetic imagery away.
- **Develop strong security protocols**: Include AI-driven threat-detection, identity-verification and cyber-defence systems to protect digital-ID infrastructure. Capabilities such as biometric anti-spoofing (the technologies deployed in biometric systems to prevent criminals or impostors from spoofing the process using photographs, videos, masks or other non-living artefacts) and behavioural analysis can enhance security. Continuous monitoring and regular updates are vital to stay ahead of emerging risks. Multi-layered security approaches are generally favoured.
- **Prioritise accessibility and inclusion**: Ensure digital-ID services are accessible to all, addressing bias and inclusivity. Provide 24/7 remote access and seamless enrolment, even in underserved areas. Avoid reliance on expensive devices or complex actions that can exclude users. Governments must avoid unintentionally excluding people by discontinuing legacy processes too quickly.
- **Encourage innovation ecosystems**: Foster innovation by setting up "sandbox" challenges for innovators to address and scale. The EU Digital Identity Wallet pilot (underpinned by eIDAS 2.0) is a great example, giving rise to digital-ID projects such as POTENTIAL and NOBID. Governments should support startup communities and create environments where new ideas can be tested and developed with regulatory support.
- **Foster international collaboration**: Cyber threats, digital manipulation and identity fraud are global issues requiring international cooperation and knowledge sharing. Governments should collaborate through initiatives such as the Global Partnership on Artificial Intelligence, SIDI Hub and UNICEF's Digital Public Goods Alliance to develop standards, share practices, promote interoperability and coordinate strategies.

Conclusion

The integration of AI into digital-ID systems holds immense potential to transform public-service delivery, enhance efficiency, improve cyber-security and promote inclusivity. This is no longer a distant, possible future; it is an imminent reality that must be shaped responsibly and proactively.

Governments must leverage AI's capabilities and implement robust security measures and regulatory frameworks to ensure that digital-ID systems are secure, trustworthy and beneficial for all citizens. By addressing the challenges of deepfakes, remote transaction manipulation and data protection head on, nations can harness digital-ID innovation and AI capabilities responsibly and unlock extensive benefits: personalised education, improved health care, seamless access to services and data-driven policymaking.

Governments can foster a future where citizens exercise greater control over their personal data and enjoy an inclusive, empowering digital experience. They must insist on the highest standards of transparency, privacy protections and individual control without failing to reap the benefits of this critical technological moment.

The stakes are high but so are the potential rewards. As stewards of this transformative change, governments must seize the opportunity to leverage AI's potential while safeguarding against its risks, paving the way for a digitally empowered society that leaves no one behind.

TONY BLAIR
INSTITUTE FOR
GLOBAL CHANGE

Follow us

facebook.com/instituteglobal
x.com/instituteGC
instagram.com/institutegc

General enquiries

info@institute.global