JULY 2023

YIANNIS THEODOROU

Ten Actions Countries Should Take to Create a Digital-Identity Ecosystem

TONY BLAIR
INSTITUTE FOR
GLOBAL CHANGE

Every country faces unique challenges on the road to establishing a digital-identity system, and some are further ahead than others. As our recent paper *The Great Enabler: Transforming the Future of Britain's Public Services Through Digital Identity* examines, some countries have a political battle to win before advances can be made. But research from Deloitte indicates that people are more in favour of digital identity than opposed, particularly when the benefits are made clear and security and privacy are priorities.

A digital identity can enable individuals to participate in the digital economy and access government and many private-sector services remotely. If designed properly, it can also give people greater control over their data. For example, an individual should only have to share the identity-related information that is pertinent to the action they are taking; a pharmacist issuing medication only needs to know that a person has a valid prescription, rather than requiring other credentials like age or address.

More broadly, a well-designed digital-identity system could revolutionise how people interact with public services – education, health care and welfare, for example – and enable government to move at a pace fit for the 21st century. It would bring speed and efficiency while generating insights to drive improvement and innovation, underpinning a new "strategic state" that harnesses technology to provide better services and empower individuals.

There are ten core actions that governments can take to set up a fit-for-purpose, trusted and widely adopted digital-identity ecosystem. However, there is no one-size-fits-all approach to implementing these actions. The Tony Blair Institute for Global Change's (TBI's) recent three-country study in Africa, *Digital ID Can Help to Better Serve Marginalised Groups in Society*, showed there is merit in digital-identity systems that cater for the needs of specific groups.

These ten steps can serve as the foundation for planning digital-identity systems.

1. Make Digital Identity a Top-Level Priority and Create a Delivery Roadmap

The number of stakeholders involved in establishing a well-functioning digital-identity ecosystem means that strong coordination and buy-in is needed from the outset. The mandate should come from the prime minister or president and progress should be closely monitored at top levels, ensuring actions are taken swiftly and decisively.

A government leader can achieve this by making digital identity a priority of a high-level ministerial or presidential delivery unit or appointing a senior champion who answers directly to the head of state.

Consulting with the public and private sectors is vital to ensuring a full understanding of the available technologies that the system will rely on and assessing how solutions or design approaches would meet the government's needs.

2. Assess Existing Identification Systems

Most countries have several identification databases already so there is often no need to start from scratch when creating a population registry. Governments should evaluate what's already available by commissioning a cross-governmental assessment of existing identity and civil registries, looking at recognised identity databases and documents such as passports, birth certificates, driving licences, as well as social security or tax identifiers. To the extent they are deemed to be robust, these government-recognised registries (machine-readable identity documents) could be leveraged to derive digital-identity credentials and attributes that could unlock access to online services.

Broader infrastructure questions need to be explored too. Looking at levels of smartphone adoption, for example, offers a route to easy enrolment by leveraging a smartphone's camera to verify identity. But it is also vital that governments account for groups who are at risk of being excluded from systems to avoid further entrenching digital inequalities.

3. Strengthen National Digital Infrastructure

A digital-identity ecosystem can only be truly inclusive and robust when underlying foundations are in place. These include:

Internet connectivity, which is vital for universal coverage. As TBI's work in Zambia, Malawi and most recently in Rwanda with Starlink has shown, satellite internet technology can now make this a possibility even in the most remote regions where mobile internet is unavailable and laying cable logistically unfeasible.

Reliable and secure data storage. Whether it's cloud or local data centres, reliable and secure data storage is vital because governments need flexible data-resiliency and back-up arrangements in place to ensure data are always available and accessible despite unexpected disruptions such as power cuts, cyber-attacks or invasions.

Data security and cyber-security protocols. National public key infrastructure must be in place, as well as a comprehensive data-governance framework. These protocols must exist to ensure the principle of security-by-design is built into national digital-infrastructure safety in an end-to-end manner.

4. Integrate Multiple Registries

Secure national digital infrastructure can link population registries with civil registries and help de-duplicate foundational identity records. For example, it can link a birth-certificate record to a national identification record and ensure that everyone appears only once in the population registry. This marks a significant step towards creating robust digital-government portals, streamlining processes and limiting bureaucracy.

However, integrating registries does not mean everything has to be linked to a single identity number; rather, that the foundational identity can act as the source of truth through which service providers, such as a driving-licence authority, a national tax body or a national health service, could verify an individual's identity and issue unique credentials to that person.

5. Issue Verifiable Digital Identity

Whether via a smartcard (a card with a machine-readable chip), a mobile identity or a QR code, a digital identity needs to be verifiable in line with existing or emerging international standards for it to unlock access to vital services. Verified claims, which provide assured identity information, play a crucial role in terms of allowing people and organisations to trust identity information online, but details and standards relating to sharing this information between "issuers", "holders" and "verifiers" are still being developed.

Countries will differ in terms of their approach to verifiable digital identity and currently there is no single solution. Factors like levels of smartphone adoption, internet coverage and rates of digital literacy play a role. In many countries with a high degree of smartphone ownership, going fully digital is a realistic aspiration, but in countries in which fewer people have smartphones, a smartcard option linked to a verifiable set of identity credentials (in person or online) will still transform lives.

6. Open Up Enrolment to Ensure Inclusivity

Having a robust digital-identity ecosystem is not enough; it should be inclusive. This raises key questions. How easily can a person access a digital identity? Does the process cater for traditionally marginalised groups such as older people, rural residents, people living with disabilities or refugees and migrants? If biometrics like fingerprint capture are involved, does the onboarding process accommodate everyone? For some people – such as manual workers with calluses on their fingers – fingerprint capture or verification will simply not be an option.

There are various ways of making enrolment processes inclusive, from onboarding existing identities into a mobile identity scheme to issuing an entirely new identity which is not restricted to a single biometric modality and capturing a minimum set of biographic information such as name, date and place of birth, and parents' names. Either way, enrolment campaigns and processes constitute a fundamental part of the success; the more they cater for marginalised groups, the more inclusive they will be.

7. Create Strong Governance and Legal Frameworks

Creating fit-for-purpose legal and policy frameworks is a huge area of work but there are three core components that are particularly noteworthy: establishing data protection and privacy laws that comply with local and regional regulations and international best practice; having laws that set out appropriate regulatory oversight and audits; and ensuring there are clear mechanisms for redress so that people know where to go if they encounter problems.

8. Set Up a Trust Framework

An optimal digital-identity ecosystem requires many actors and roles. A trust framework is a rulebook that all ecosystem users should adhere to. It defines who is part of the ecosystem and how they can formally join, and identifies the identity issuers, verifiers and other parties. Rules should state which standards bodies are involved from each industry and how they should create uniform approaches for participants.

These frameworks should detail how an auditor would assess the adequacy of system controls and recommend changes, as well as how the relevant regulators implement and enforce compliance at domestic, regional or international levels.

9. Enable Impactful Use Cases and Invest in Building Digital Skills

Use cases – the scenarios in which a product or service is used – are what turn digital identities into a rich ecosystem. Valued use cases may differ across countries.

If a country has large agricultural regions, then governments should look at ways in which a digital identity could help farmers the most – for example, by allowing them to verify their eligibility for fertiliser subsidies linked to the size of their land. This would act as an impactful use case, directly benefiting farmers' livelihoods while reducing inefficiency. In urban locations, using digital identity to facilitate onboarding for banking services tends to be a prevalent use case.

Governments should prioritise the creation of digital-identity use cases that maximise value to people's lives, especially when trying to reach a subset of the population.

10. Achieve Interoperability

The final step is to ensure identity verification across borders. To do this, countries should strive to use interoperable standards when building digital-identity systems.

When looking at the International Civil Aviation Organization standard that passports comply with, it's easy to grasp how important it is for an identity credential – linked to international travel – to be interoperable across borders. Extending the same principle to national digital identities would also facilitate freedom of movement and employment where permissible, for example, within regional blocs such as the European Union.

Governments should aim to be part of a global community that shapes development and standards, and enables digital identity to transform lives, save time and give more control over personal data.

Conclusion

While innovations in the private sector are ahead of the public sector, governments are steadily realising two things: firstly, that a robust digital-identity system is a core enabler of a strategic state which can deliver efficiencies, better governance and personalised services; and secondly, that fast-paced developments in the artificial-intelligence space mean there is increasing need to protect people's identities online and mitigate risks posed by "deepfakes" and identity fraud more broadly.

The momentum behind harnessing the potential of digital identity is stronger than ever.

Lead image: Getty

TONY BLAIR
INSTITUTE FOR
GLOBAL CHANGE

Follow us

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

General enquiries

info@institute.global