DECENTRALISED IDENTITY SYSTEMS

A Strategic Framework for Government Digital Transformation

Whitepaper

TOPPAN
TOPPAN Security

WHAT IS DECENTRALISED IDENTITY?

Decentralised identity, in the context of this paper, refers specifically to digital identity implemented through verifiable credentials (VCs) which is a fundamental shift in how personal information is managed in the digital age. Unlike traditional systems where governments or corporations store and control citizen data in central databases, decentralised identity places individuals at the center of their own identity management (self-sovereign identity or SSI).

Citizens hold their credentials in secure digital wallets or SuperApps on their personal devices, deciding when, how, and with whom to share specific pieces of information.

A decentralised system operates through four key components:

1. Issuers: trusted authorities (such as government agencies) that create and certify verifiable credentials.

2. Digital Wallets or SuperApps: secure applications on citizens' devices for storing and presenting credentials.

3. Trust Registries: authoritative records that allow relying parties to verify the legitimacy of issuers.

4. Relying Parties (RPs): services or organizations that accept and verify credentials such as a hotel checking you in.

When citizens need to prove their identity or qualifications, they can share only the specific information required (selective disclosure). Instead of revealing full personal details, they provide attestations (data minimization), for example, proving they live in a certain city without sharing their full address, or confirming they are over 18 without disclosing their exact date of birth. This selective disclosure and data minimization protects privacy while maintaining trust.

CENTRALISED SYSTEMS: A SINGLE POINT OF FAILURE

Centralised identity systems concentrate all citizen data in government-controlled databases.

While this approach offers administrative simplicity, internet-facing databases with citizens personal identity information is a prime target for hackers, making centralised systems a single point of failure.

In centralised systems, maintaining the high availability and reliability required to support private sector activity and government services is costly, and those costs continue to rise as adoption increases. These systems also concentrate control in a single authority, creating risks of surveillance, exclusion of marginalized groups, and misuse or sale of citizens' personal data.

DECENTRALISATION: DISTRIBUTED BY DESIGN

Decentralised systems ensure that the citizens can prove their identity to a relying party without the government being involved in the transaction, allowing it to grow acceptance while the cost remains steady. Decentralised systems could also offer new revenue streams.

With decentralised systems the government has the data stored in a central system but that database is not internet-facing as citizens can receive a digital signed copy of their data in their application. Since data is stored on citizens' devices rather than central servers, there is no honeypot for hackers to target. Verification occurs through cryptographic proof rather than database lookup, enabling offline functionality in areas with limited connectivity. The distributed architecture eliminates single points of failure and reduces infrastructure costs. Most importantly, citizens retain sovereignty over their own data, building trust in government systems while protecting privacy.

	Centralised	Decentralised
Credential Storage	Stored on server	Distributed in users' wallet
Single Point of Failure	Yes	No
User Data Security	★☆☆	★★★
Citizen Data Privacy	☆☆☆	★★★
Citizen Data Control	★☆☆	★★★
Verification Mode	Online	Online and Offline
Costs and Scalability	Expensive	Efficient
Interoperability	Not interoperable	International standards
Inclusivity	★☆☆	★★★

WHY DECENTRALISED IDENTITY IS THE BETTER CHOICE FOR GOVERNMENTS

For governments, decentralized identity offers compelling advantages.

McKinsey estimates digital identity systems could unlock 3–13% of GDP in economic value by 2030 for emerging economies.

For governments with limited budgets, the reduced infrastructure requirements and vendor-neutral architecture grounded in international standards prevents costly lock-ins to proprietary solutions and ensure long-term interoperability across borders and services.

VERIFICATION WITHOUT CENTRAL DEPENDENCE

Online And Offline is Possible

A decentralised identity ecosystem allows people to verify who they are in different situations. Credentials are shared directly from a citizen's digital wallet to the organization requesting them. Verification happens using cryptographic proof, not by checking a central database. This approach works both online and offline, which is especially important in areas where internet access is unreliable or uneven.

To make the system inclusive, access must be carefully considered. It should work for people who own a smartphone as well as for those who share one. It must also support people living in areas with little or no connectivity, and services should continue to function even when the internet is down. For this reason, offline features and flexible wallet options are not extras, they are essential for a fair and equitable rollout.

Private Sector Engagement

Private sector involvement is essential for the success of the ecosystem. Banks and mobile money operators can use the system for streamlined KYC processes greatly simplifying the user experience for identity documents to be captured and reducing onboarding time to a few seconds.

Telecommunication companies can integrate SIM registration with digital identity verification. The key is establishing clear standards and certification programs that allow multiple providers to participate while maintaining security and interoperability.

It is worth noting that the verifiable credential framework can also support a broader range of use cases beyond national digital identity such as professional qualifications, licenses, or other attestations. These represent distinct credential types built on the same infrastructure and should be understood as extensions of the ecosystem rather than components of identity itself.

GOVERNMENT OPPORTUNITIES

The digital ecosystem between citizens, government, and the private sector, enabled by decentralized identity, also presents an opportunity for governments to open new revenue streams. By adopting internationally recognized standards, governments can further facilitate cross-border digital transactions, expanding the commercial opportunities available to businesses and, in turn, growing the tax revenues that flow from increased economic activity.
Taking the EUDI (European Digital Identity) Wallet as an example, European governments are placing regulatory requirements on the private sector to verify citizens' digital identities across a range of use cases.

These include access to social media platforms (restricted to users above a minimum age that varies by country) and the online purchase of age-restricted goods and services, such as alcohol. As a result, age verification emerges as a high-frequency use case, requiring citizens to prove their identity on a regular basis.
This dynamic creates an opening for governments to introduce fee structures for private sector entities connecting to the system, whether as a flat access fee or on a per-verification basis, potentially tiered by transaction volume and enforced through regulation.

Governments can implement these revenue models through verifier authorization.
All verifiers are authorized through authentication certificate that comes with expiration, providing a mean to enable and enforce subscription. Yet not tracking individual transactions but ensuring recurring revenue through license renewals.

Additionally governments can authorize verifier technology that enforces prepaid transaction limits and can further report transactions. Private sector entities such as telecom operators conducting SIM registration verification and banking institutions performing customer onboarding can purchase a specific number of verifications upfront, similar to existing KYC licensing models. These verifiers can be shut down (not renewed) when reporting is not received.

Reporting can be structured as daily or monthly summaries rather than real-time monitoring, balancing government visibility needs with system efficiency. Compliance can be enforced by automatically disabling verifiers that fail to submit required reports, ensuring adherence to authorized usage terms while maintaining the system's decentralized benefits.

RECOMMENDATIONS FOR GOVERNMENTS

For governments at the beginning of their digitization journey, we recommend:

- Establishing a robust legal and data protection framework before deployment.
- Selecting solutions built on international open standards to guarantee interoperability and avoid vendor lock-in.
- Engaging civil society to build public trust and ensure citizen rights are embedded in the system design.
- Prioritizing mobile-first and offline-capable design to maximize inclusion.

The path to decentralised identity represents not merely a technological upgrade, but a fundamental reimagining of the relationship between citizens and the state: one built on trust, privacy, and individual empowerment.

TOPPAN

TOPPAN Security

www.toppansecurity.com
info@toppansecurity.com