Digital IDs — the good, the bad and the ugly

Credit: Claudia Pizzocri, Daily Maverick



Leon Schreiber

Home Affairs Minister Leon Schreiber recently announced that the Department of Home Affairs (DHA) would submit a Digital ID policy to the Cabinet to enable public consultations. Shortly afterwards, the MyMzansi "digital public infrastructure" (DPI) roadmap was unveiled: a single digital ID, a data-exchange platform and digital payments layer. In practical terms, this envisages a state-controlled data spine linking Home Affairs, revenue, social grants and other core systems, with the digital ID acting as the key that unlocks those rails across public and private services. The pitch is attractive: one secure identity to access state services, social support, financial products and private platforms, all from your phone; less queuing, less fraud, less paperwork and more dignity for all.

The good

A well-designed digital ID can reduce transaction costs for people who already exist clearly in the system and deepen inclusion for those who struggle to prove themselves, over and over.

The EU model, at least on paper, constrains itself: voluntary wallets, multiple credentials, explicit data-minimisation duties, strong links to an independent data-protection regime. Used this way, a digital ID becomes an instrument people deploy, not a leash the state tightens.

A South African model aligned to the Protection of Personal Information Act (POPIA), Promotion of Access to Information Act (PAIA) and the Constitution's guarantees of dignity, privacy and equality as real design constraints, not afterthoughts, could, in principle, do something similar: a credential that people turn on and off, and that is tightly limited in what it may reveal and to whom.

South Africa would greatly benefit from a similar implementation as its systems still heavily depend on fragile documents and brittle, poorly integrated databases. A coherent, secure way to authenticate identity across banks, schools, hospitals and borders could, in theory, help unwind fraud, impersonation and administrative error.

It could support a rights-anchored infrastructure of documentation, where the state's records are reliable enough that people are not forever challenged on their own existence.

The bad

Digital IDs also centralise risk. They create attractive targets for criminal intrusion and for internal abuse. Where technical architecture, vendor contracts and security audits are shielded by opacity, the public is effectively asked to outsource trust to actors who can be weakly accountable. Long-term, opaque procurement and public-private partnerships can entrench a handful of vendors as de facto gatekeepers of the country's identity rails, leaving government and the public paying, in effect, for access to information that should already be theirs.

South Africa's record here is sobering. From the aborted "Who Am I Online" overhaul, the tainted Abis biometric backbone, to the unlawful and dependency-creating Sassa–CPS grants arrangement, core identity and welfare functions have repeatedly been embedded in proprietary systems that the public and Parliament could not meaningfully inspect.

Each of these projects promised modernisation and efficiency; each left behind a pattern of overselling, underdelivery and deep dependence on private infrastructure for core public functions.

Unless anchored in statute, practice and public oversight, a single digital ID and DPI stack on top of that history would entrench those defects rather than repair them, especially if there are no clear legal limits on purpose, no routine publication of independent security audits and no simple, fast remedies for people who are wrongly flagged or cut off.

Digital IDs also intensify exclusion in less visible ways. Systems built around stable connectivity, device ownership and clean underlying records will predictably work best for those closest to the administrative norm.

Without enforceable guarantees of equivalent non-digital routes, the digital ID becomes a gate that works seamlessly for the already legible, and intermittently or not at all for those whose documentation is partial, complex or contested.

The ugly

In the absence of a genuinely parallel, functioning non-digital route, "voluntary" digital identity schemes tend to become effectively compulsory over time. The risk increases to that of purposeful marginalisation of those who simply do not want to conform because they might not trust the tools and who controls them.

In the UK, the link between digital ID, immigration control and employment is explicit: the system is justified in part as a way to prevent those without the "right" status from working. The identity spine is engineered with exclusion as a core function, not a side-effect.

A similar South African pattern would not be difficult to imagine: digital ID becoming the default rail for work authorisation checks, SIM registration or basic banking, with non-citizens and anyone with a complicated status finding themselves locked out of all service functionalities simultaneously.

Across Europe, the pattern is more layered, but structurally similar. Schemes framed as voluntary become, over time, practically indispensable for full access to e-government and many private services.

Italy's recent move to phase out legacy ID cards as valid travel documents in favour of high-security electronic credentials illustrates how quickly technical upgrades can translate into structural reliance.

A South African version is not hard to sketch because parts of it are already on the table. In July 2025, Schreiber outlined a timetable to stop issuing green ID books by the end of 2025 and to discontinue them entirely by 2029, while rapidly expanding smart ID card issuance through new live-capture systems and bank branches.

That is framed as a necessary anti-fraud and access measure. But once a digital ID wallet sits on top of that infrastructure, it is easy to imagine the physical documents slowly becoming second-tier, accepted in fewer and fewer contexts as the digital ID is treated as the "real" key, with those who cannot or will not use it pushed to the edges of legality and convenience.

Once a digital identity backbone exists, attaching new functions to it becomes technically trivial and politically tempting, and reversing course becomes difficult.

The cliché is to warn of an Orwellian surveillance state. The more likely outcome is less theatrical and more corrosive: an infrastructure that quietly makes existing power easier to exercise and harder to resist.

Once access to work, banking, movement and basic services runs through a single, networked identity spine, any error, flag or discretionary status change can lock a person out across multiple systems at once. A mistaken fraud marker, entered once into a shared system, could mean a suspended social grant, a frozen bank account and a blocked permit renewal, with the affected person shuttled between institutions that all point to the same invisible status code.

Where do South Africans stand on the issue at the moment

If South Africa is to proceed into its self-declared "digital era", the real choice is not between embracing or rejecting technology. It is between models: whether we build an infrastructure that is explicitly constrained by constitutional limits and plural lives, or one that quietly equips the state to deal more swiftly and severely with anyone who falls outside the format it prefers.

A constrained model would hard-wire legal guarantees of non-digital access, strict limits on what data the digital ID may reveal and for what purposes, independent and technically competent oversight, and particular protections for migrants, refugees and others whose status is most easily weaponised.

But, at the end of the day, it's what South African sentiment is toward digital IDs, Right now, South African sentiment is deeply divided. There is widespread relief over efforts to reduce bureaucratic

inefficiency, coupled with strong concerns over data privacy, cybersecurity, and the potential for digital exclusion.

The spectrum of public opinion breaks down into two main views:

Broad support for convenience and inclusion

Many South Africans enthusiastically welcome digital alternatives, primarily because it offers a way to bypass the notoriously long queues and administrative delays at Department of Home Affairs (DHA) branches.

Citizens largely trust digital identity verification in the banking sector (such as biometric logins on apps and liveness checks) as a secure, normalized way to prevent fraud.

The government's push to make Smart ID cards and digital wallets more accessible—such as the in-branch partnerships rolling out at Capitec and other banks—has been celebrated as a major step forward for inclusive governance and expanding financial access.

Growing concerns over privacy and exclusion

Public research, such as CSIR surveys, shows that a large majority of citizens foresee privacy violations and worry about cybersecurity, especially regarding how consolidated biometric data will be stored and used.

Critics, including researchers at Research ICT Africa, warn that consolidating identity and service access on a digital platform could lock vulnerable, remote, or undocumented South Africans out of essential state grants and civic services.

In conclusion

Advocacy groups and privacy advocates have raised alarms about government overreach, citing historical issues where state databases were mismanaged or used improperly.

The wider consensus is that citizens welcome the benefits of digital IDs, such as convenience and security, but there is an insistent demand for clear legislative guardrails to protect privacy and prevent authoritarian abuse. The Department of Home Affairs is actively taking public input on the regulations governing the "Mzanzi" digital ID system to address these concerns before it is finalized

--ooo--