View on Web

How Governments Can Build Trusted Digital Identity Systems

29th Sep,2026

A digital identity system is more than a digital ID card. It is the trust layer of a digital government. When citizens use one identity to access healthcare, welfare, banking, licenses or public services, governments are effectively asking them to trust an invisible infrastructure with some of their most sensitive information.



That trust cannot be downloaded. It has to be engineered.

McKinsey notes that governments have launched 165 digital or partially digital ID schemes globally, yet adoption and usage varied sharply. Its analysis found that some schemes were used only once or twice a year, while successful systems created a virtuous cycle in which useful services attracted citizens and citizen adoption encouraged more service providers to participate.

So, how can governments build trusted digital identity systems?

Make privacy the default: Digital identity should follow data minimization: collect only what a transaction genuinely requires. The World Bank's ID4D (Identification for Development) framework recommends privacy and security by design, including encryption, tokenization, distributed processing and user control. Meronymity- Taiwan's selective disclosure approach, illustrates how identity can prove eligibility without unnecessarily exposing an entire personal profile.

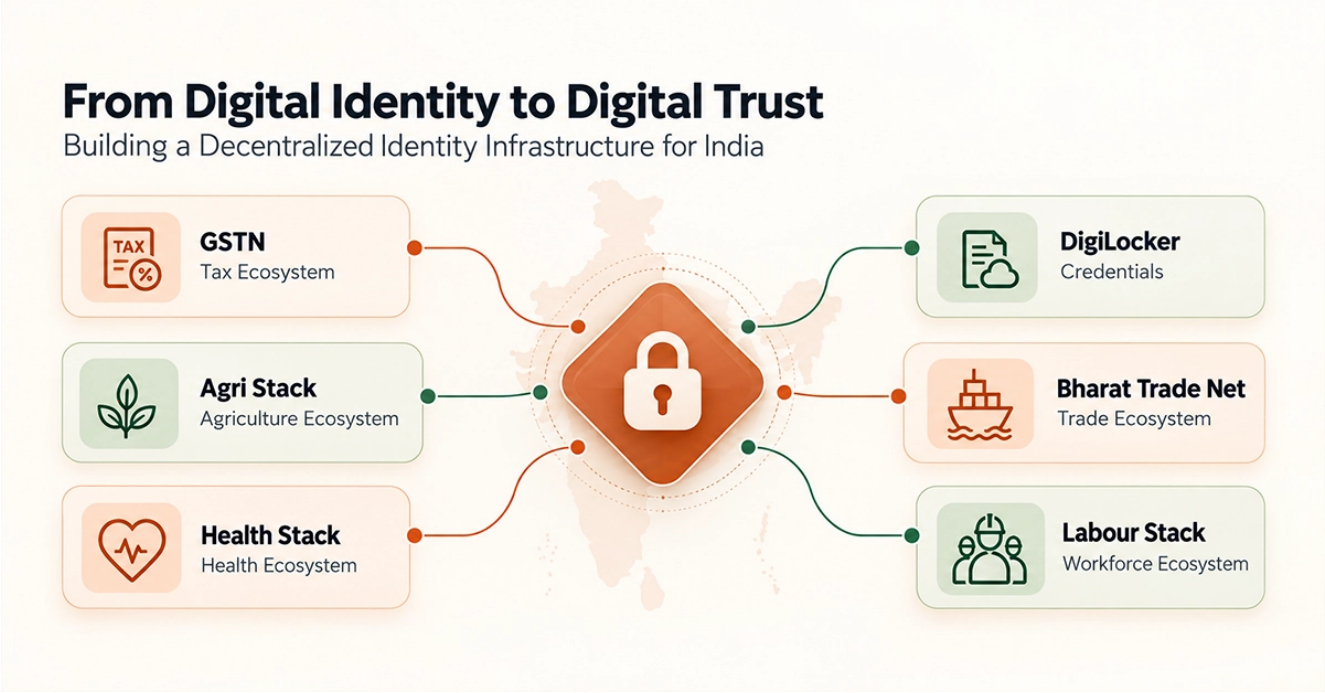
Build interoperability, not digital islands: An identity system becomes valuable when it can securely work across government databases, private services, applications and jurisdictions. The World Bank identifies interoperability and open standards as core design principles. The EU Digital Identity Wallet similarly relies on common standards so citizens can authenticate across borders and services.

Create strong legal guardrails: Governments need clear rules defining what data can be collected, why it can be used, who can access it, how errors can be corrected and where citizens can seek redress. The World Bank stresses comprehensive legal frameworks, institutional accountability and independent oversight.

Design for real-life usefulness: A digital identity that has nowhere useful to go will remain an expensive credential. McKinsey found that Sweden's BankID generated about 91% of its use cases from the private sector, demonstrating the importance of combining public and private services.

Treat User Experience (UX) as infrastructure: Enrollment must be simple, authentication proportionate to risk, and services accessible to people with different levels of digital capability. Inclusion is not an optional feature: the World Bank places universal coverage and accessibility at the foundation of trusted identification.

The critical lesson is simple- digital identity should not become a database of citizens; it should become a trusted mechanism for citizens to prove what is necessary, when necessary.



Identity at Scale: How CSM Powers Trusted Digital ID Systems

Governments don't need another authentication tool- they need identity built as foundational infrastructure. That's where CSM Technologies delivers.

As an official system integrator on the **MOSIP** marketplace we architect vendor-neutral, modular ID platforms nations can truly own. Our privacy-by-design approach, including secure data vaults for biometrics ensures that citizen trust isn't an afterthought, it's the foundation.

We don't stop at issuance. Our lifecycle management secures identity from creation through retirement, while interoperable service layers connect welfare, taxation, and labor departments seamlessly.

Proof, not promises: our **Odisha Aadhaar Authentication Framework (OAAF)** has processed over 1.14 billion authentications at population scale, under real-world pressure. The result is invisible governance: AI-driven authentication working quietly behind every citizen interaction.

If your government or agency is weighing how to modernize digital identity, evaluating vendors, or trying to move a stalled ID program toward real adoption, this is the conversation worth having.



The future: identity people can control

Governments should now move from identity systems built around institutional convenience to citizen-controlled, privacy-preserving and interoperable digital identity ecosystems.

The next generation of digital government will not be defined by how much information the state possesses, but by how intelligently and responsibly it enables people to use their own identity.



AUTHOR:

Jayajit Dash

Senior Manager- Corporate Communications (Marketing)

© Copyright CSM Technologies, Level-6, E/56, Infocity, Chandrasekharpur, Bhubaneswar, Odisha - 751024