

# From Scale to Standards: Building a Global Digital Identity Standards Ecosystem

– Isha Chaudhari (IIT Gandhinagar)



MOSIP Connect 2026 • Rabat, Morocco

# From Scale to Standards

Building a Global Digital Identity Standards Ecosystem

12.02.2026

For Discussion Purposes Only



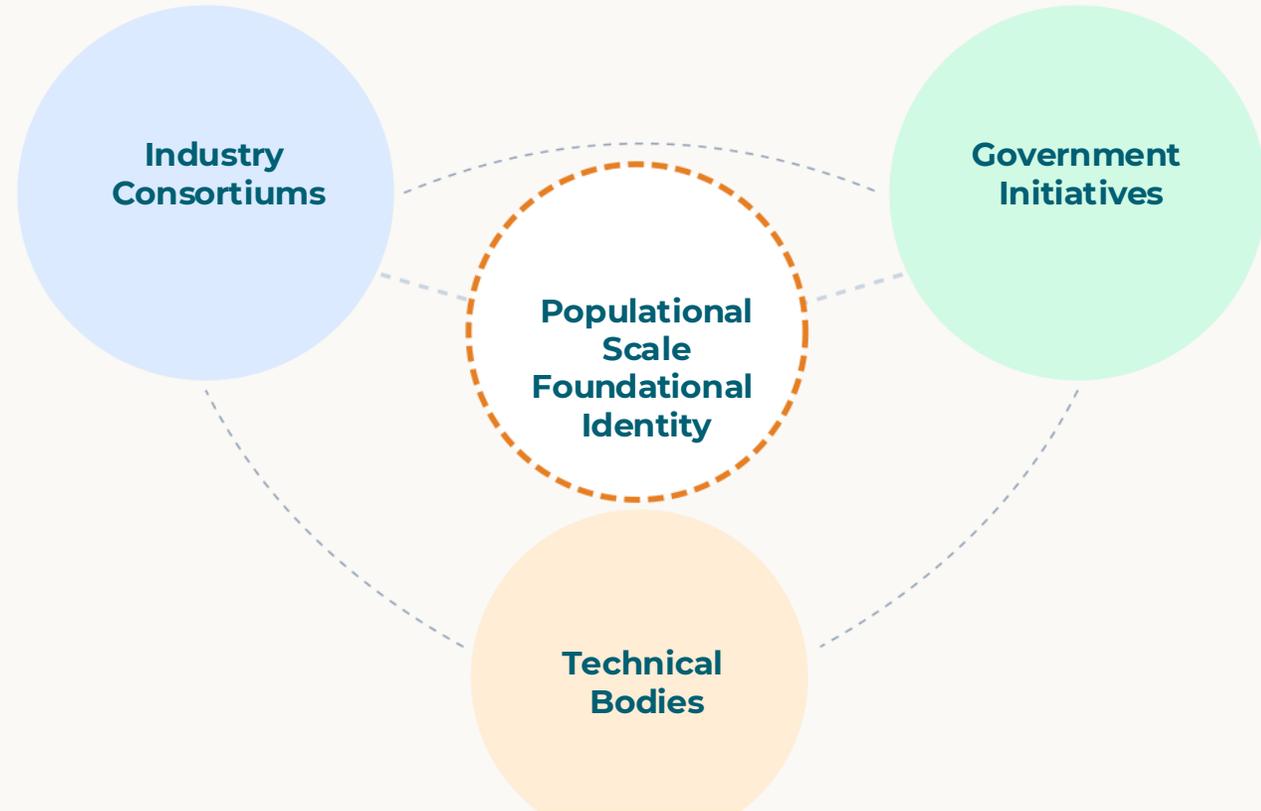
Strategic Vision

# Why?

Building a resilient, inclusive, and interoperable digital identity ecosystem for the future.

## The Current Landscape Void

We need to bridge this void between optimization, regulations, and technological development.



### Prevent Vendor Lock-in

Steward towards **Open Standards** for sustainability.



### Domestic & Regional Growth

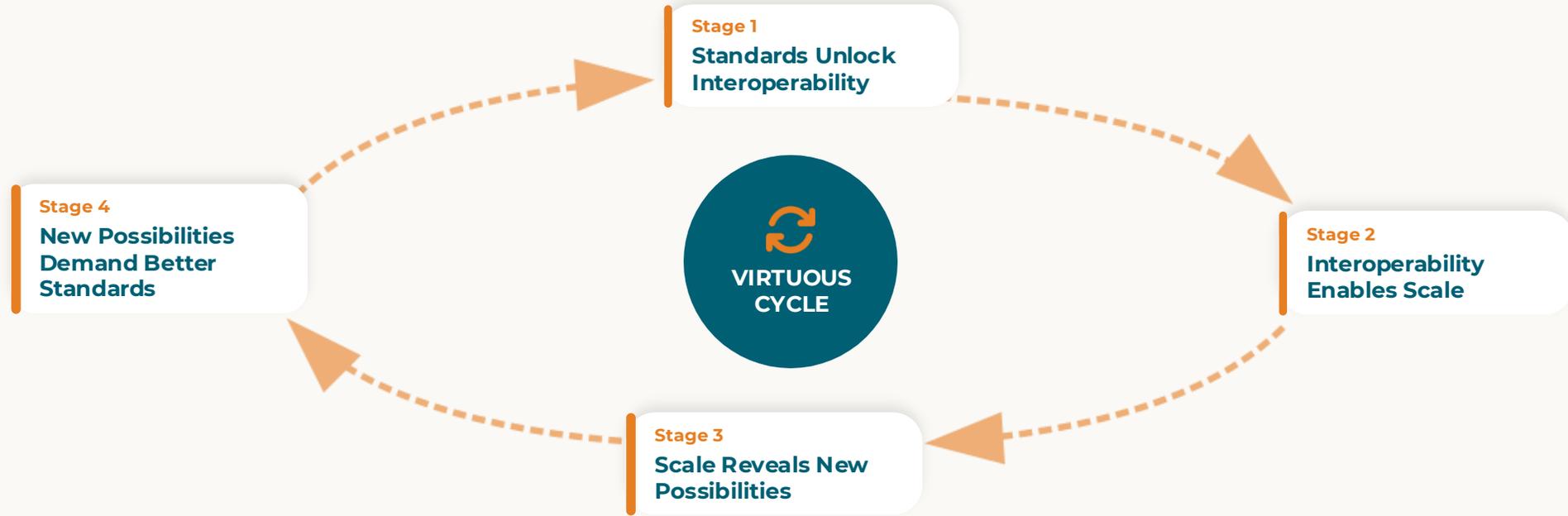
Create a **Level Playing Field** for local ecosystems.



### Strategic Autonomy

Provide for **Sovereign Needs** while maintaining interoperability

# Why Standards?



"Each rotation makes the next one easier and faster."

<p> <b>Solves Chicken-Egg Problem</b> Not enough customers = no services services to use. Standards break the break the deadlock.</p>	<p> <b>Combinatorial Innovation</b> Standardized building blocks allow allow innovators to combine them them in unexpected ways.</p>	<p> <b>Democratizes Innovation</b> Levels the playing field for all participants, not just large players. players.</p>	<p> <b>Long-Term Investments</b> Stable foundations enable sustained sustained R&amp;D and infrastructure infrastructure development.</p>
--	---	---	--

# The Scale of the Opportunity

**850  
million**

People worldwide still lack legal identity.



Sustainable Development Goals depend on inclusive identity systems.

**40+**

Countries are actively building or planning foundational digital ID.

---

**Interoperable standards could accelerate every one of these efforts.  
Without them, each country reinvents the wheel—alone.**

# Standardisation Focus



## Data Models

Promoting interoperable formats and common schemas to ensure functional IDs are understood across systems.



## Consent & Privacy

Architecting standardized consent mechanisms giving users granular control over their functional credentials.



## Exchange Protocols

Standardizing protocols for issuing, presenting, and verifying credentials for seamless verification.

## 🎯 Initial Focus Areas



### Sovereign Identity Systems

Establishing foundational national infrastructure for authoritative identity authoritative identity management, legal recognition, and population-scale operations.



### Identity Chains

Creating interoperable linkages that enable credentials to flow securely across borders and sectors, bridging foundational and functional IDs.

# Sovereign Identity Systems

## Definition

A Sovereign Identity System comprises the technical infrastructure, protocols, and governance mechanisms through which a country establishes, maintains, and authenticates the identity of individuals under its jurisdiction.



### Authoritative Identity Establishment

Government-issued credentials carrying legal recognition and evidentiary weight in administrative, administrative and judicial proceedings.



### Population-Scale Operations

Technical architectures capable of managing billions of records with sub-second authentication response times.



### Biometric Deduplication

1:N matching across entire population databases to ensure uniqueness of issued identities.



### Trust Anchor Function

Serving as the root of trust for derivative credentials issued by other government agencies and agencies and authorized private entities.

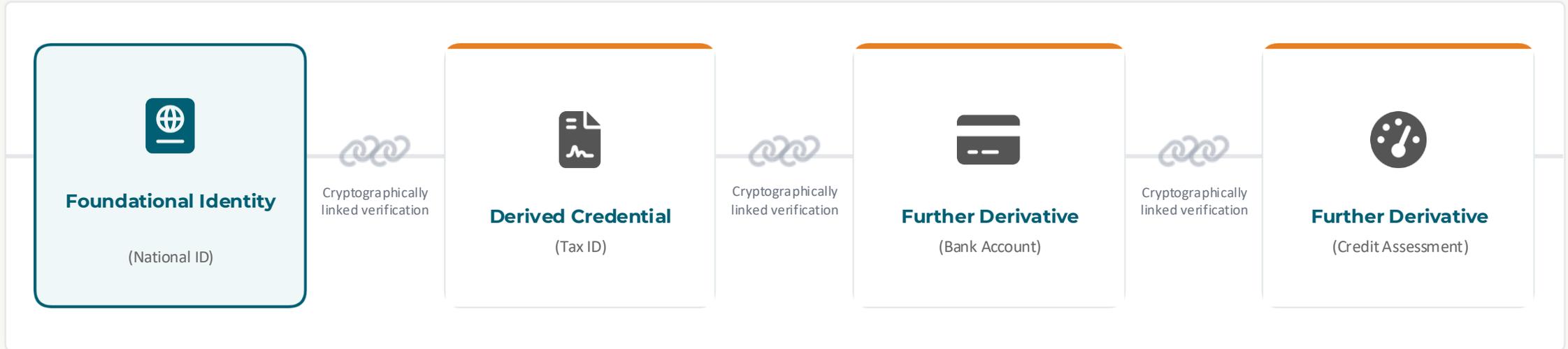


### Cross-Border Recognition

Mechanisms for mutual recognition of identity assertions between sovereign nations.

# Identity Chains

Standards for deriving, sharing, and verifying credentials across systems



### **Revocation Cascade**

When a foundational credential is revoked, how do derivative credentials learn about it?

### **Credential Transfer**

Sharing credentials between wallets—parent to child, employer to employee, temporary sharing with expiry.

### **Consent Management**

Standard formats for electronic consent, granular permissions, and revocation.

# Standards Lacuna

Identifying gaps and opportunities for DISA standardization.

★ *This list is indicative & not prescriptive*



## Sovereign Identity Space

FOUNDATIONAL LAYER

- Enrolment Quality Thresholds
- Multi-ABIS Arbitration Protocol
- Registration Packet Format
- Offline Authentication Protocol
- Sovereign-to-Sovereign Federation
- Privacy-Preserving Verification



## Identity Chains

INTEROPERABILITY LAYER

- Derivative Binding Protocol
- Chain Provenance Protocol
- Revocation Cascade Protocol
- Credential Renewal Protocol
- Delegation Credential Standard
- Backup & Recovery
- Wallet-to-Wallet Transfer
- Consent Management

# Interoperability in Action

From principles to practice • Standards enabling real-world journeys  
across borders and sectors

# Use Cases: Movement of People and Commerce



**Mary**

Software Engineer

Philippines → Dubai

Mary travels to Dubai for work. Her digital ID (ePhilID) seamlessly authenticates with UAE's systems - from airport entry to bank account setup. No additional verification needed.

Identity Chain Flow



**Salma**

Business Owner

Morocco (Verifying India)

Salma's company needs to verify Rahul's contractor credentials from India. The standardized identity chain lets her instantly verify his professional certifications, identity, and work authorization without manual checks.

Verification Flow



**Kwame**

Small Business Owner

Ghana ↔ Kenya

Kwame handles cross-border trade with Kenya. Instead of weeks of paperwork, his Ghanaian digital identity instantly verifies his business credentials and tax compliance status across African trade systems.

Trade Trust Flow



# Introducing DISA

## First effort led by country practitioners from the Global South



### Purpose

Advance practical, sovereign-aligned identity standards that solve real implementation challenges.



### Scope

Developing unified data models, consent frameworks, and exchange protocols.



### Approach

Complement—not duplicate—existing global initiatives by filling critical gaps.

# DISA Foundational Principles



01

## Strategic Autonomy

Respecting sovereign autonomy with flexible, nation led adoption path.



02

## Complement Existing Efforts

Avoid duplication by building upon established global initiatives.



03

## Open Inclusive Governance

Ensuring a democratic process where all stakeholders have a voice in shaping standards.



04

## Cross-Border Interoperability

Facilitating seamless movement of people and commerce.



05

## Vendor Neutral

Preventing vendor lock-in by defining neutral specifications that support multiple implementation and providers.



Note: Principles to be finalized in the official Alliance document.

# Who Can Join DISA



## National Identity Authorities

Teams implementing and operating foundational identity systems.



## Regional Bodies

Organizations coordinating identity initiatives across across member states.



## Open-Source Communities

Projects building identity infrastructure and tools.



## Development Organizations

Foundations and institutions supporting identity for inclusion.



## Technology Providers

Companies contributing expertise to standards development.



## Academia

Research institutions bringing rigorous evaluation and long-term perspective.

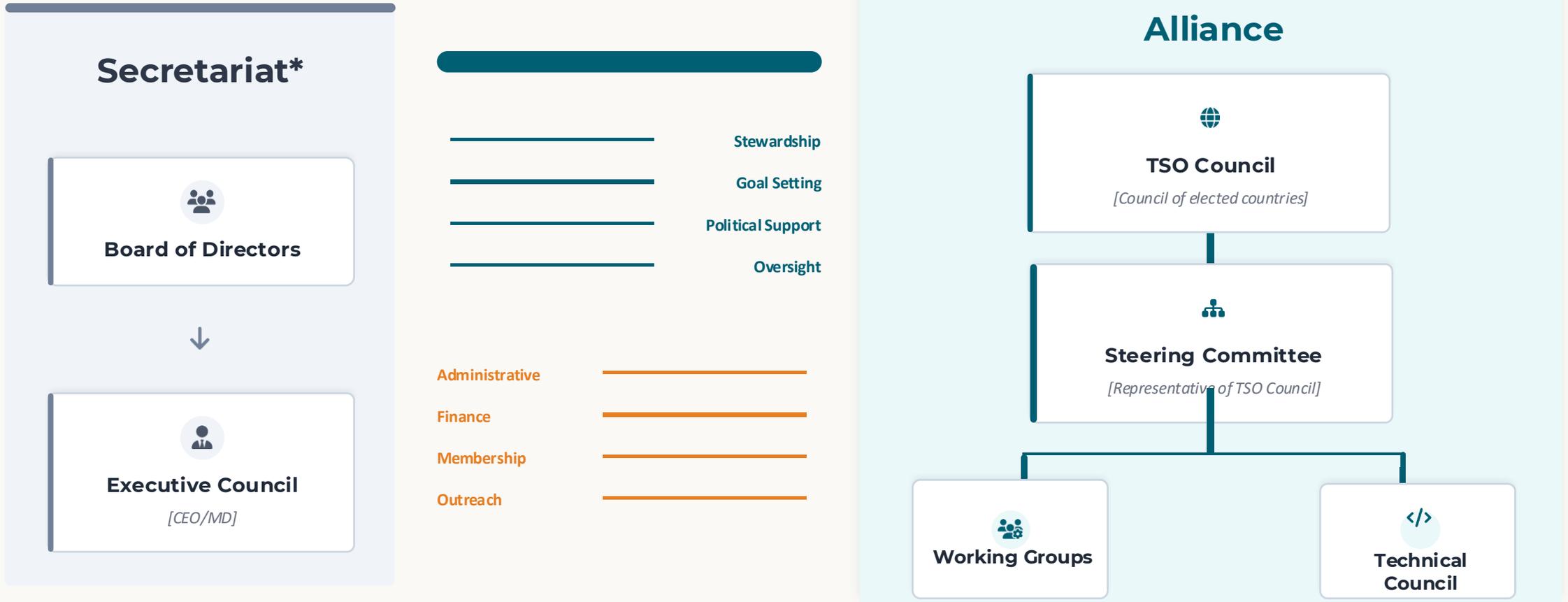


## Other ID Ecosystem Players

Additional stakeholders in the identity ecosystem.

# DISA Organizational Structure

The Alliance will be supported by a Secretariat which is a **Non-Profit Organisation**, for administrative tasks and administrative tasks and seamless operations.



Join the Conversation

# Call for Feedback & Engagement



## Comments & Suggestion

Scan to access the feedback form. Please share your interest, interest, comments & suggestions

**Contact Us**

 [ishachoudhary@iitgn.ac.in](mailto:ishachoudhary@iitgn.ac.in)

 [contact@gidso.org](mailto:contact@gidso.org)