



Le Numéro d'Identité Unique (NIU)

Arguments Pour et Contre

M. Adamou IRO

Président, HAPDP Niger | Président, NADPA/RAPDP | Ambassadeur adjoint ID4Africa

ID4Africa 2026

PLAN DE LA PRÉSENTATION

01

Les promesses du NIU

Interopérabilité, continuité du cycle de vie, efficacité

03

Alternatives au NIU

Identifiants sectoriels, modèles hybrides, systèmes distribués

05

Exemples : Inde, Estonie, Afrique

Aadhaar, X-Road, espace AES

02

Les risques et préoccupations

Surveillance, concentration du pouvoir, cyber-risques

04

MOSIP & architectures modernes

Souveraineté technologique et flexibilité des choix

06

Garanties indispensables & Conclusion

Cadre juridique, privacy by design, décision souveraine



Interopérabilité

Un identifiant unique permet aux administrations de « parler le même langage », facilite le partage d'information, réduit les incohérences et simplifie la vie des usagers.



Continuité du cycle de vie

Un individu peut être suivi administrativement de la naissance jusqu'au décès, améliorant la gestion des droits sociaux, de l'éducation et de la santé.



Efficacité des politiques publiques

Meilleur ciblage, limitation des fraudes et optimisation de l'allocation des ressources — argument particulièrement fort dans des contextes aux ressources contraintes.

→ Vu sous cet angle, le NIU apparaît presque comme une évidence.

Un NIU mal gouverné peut devenir :



Outil de surveillance systématique

Atteinte à la vie privée et risque d'abus si les garde-fous ne sont pas solides.



Dérive fonctionnelle

Extension incontrôlée de la finalité de l'usage du NIU au-delà de son objet initial.



Concentration du pouvoir

Instrument préjudiciable à la démocratie et à l'État de droit.



Guichet unique de vulnérabilité

Risques cyber amplifiés : une seule faille compromet l'ensemble du système.

→ Aucun pays n'est à l'abri. Ce n'est pas une question de niveau de développement, c'est une question de gouvernance.

Le NIU n'est pas une obligation. D'autres approches existent :

Identifiants Sectoriels

- Identifiant santé distinct de l'identifiant fiscal
- Cloisonnement des données par secteur
- Moins de risque de surveillance croisée
- Plus complexe à coordonner

Systèmes Interopérables Sans ID Unique

- Interconnexion via des protocoles communs
- Pas d'identifiant central unique
- Respect accru de la vie privée
- Gouvernance distribuée

Modèles Hybrides

- Combinaison de plusieurs approches
- Adaptation au contexte local
- Flexibilité architecturale
- Peut offrir le meilleur des deux mondes

→ Ces alternatives peuvent offrir un meilleur équilibre entre performance et protection des droits.

Qu'est-ce que MOSIP ?

MOSIP (Modular Open Source Identity Platform) est une plateforme ouverte et modulaire d'identité numérique adoptée par plusieurs pays africains dont ceux de l'espace AES.

Ses atouts clés :

- Architecture modulaire et flexible
- N'impose pas un modèle unique
- Hébergement local possible
- Indépendance vis-à-vis des fournisseurs privés
- Open source et auditable

La capacité de choix souverain

NIU centralisé

Pour les États souhaitant un identifiant unique national

Approche distribuée

Pour une gestion décentralisée respectant la vie privée

Modèle hybride

Combinaison flexible adaptée au contexte local

Que l'on adopte un NIU ou non, ces garanties sont essentielles :

1

Cadre juridique souverain et clair de protection des données personnelles

2

Approche Privacy by Design : protection des données dès la conception

3

Architecture ouverte, flexible et indépendante vis-à-vis des fournisseurs privés

4

Audit indépendant avec mécanismes de contrôle démocratique

5

Institutions indépendantes de contrôle du respect de la protection des données

6

Transparence et confiance des citoyens dans l'usage du NIU

➔ *Sans confiance, il n'y a pas de système d'identité durable.*



INDE — Aadhaar

Résultats positifs

- Identifiant unique pour +1 milliard de personnes
- Accès facilité aux services publics
- Réduction de certaines fraudes
- Inclusion financière accrue

Préoccupations soulevées

- Débats sur la protection des données
- Usages étendus non prévus initialement
- Risques d'exclusion biométrique
- Intervention de la Cour Suprême requise



ESTONIE — X-Road

Le modèle de référence en gouvernance numérique

Forte décentralisation des données

Traçabilité des accès : le citoyen voit qui consulte ses données

Cadre juridique extrêmement strict

Architecture sécurisée et auditable

Ce n'est pas l'existence du NIU qui compte, c'est la gouvernance.

01

Souveraineté et contrôle des données

- Hébergement local des données
- Gouvernance nationale des identités

02

Inclusion vs Contrôle

- Priorité à l'enrôlement massif
- Éviter que l'identité devienne un outil d'exclusion

03

Sécurité vs Libertés

- Équilibre entre lutte contre la fraude
- Respect des droits fondamentaux

04

Gradualisme

- Mise en œuvre progressive
- Tests pilotes avant généralisation

Il n'existe pas d'architecture d'identité universelle



NIU Centralisé

Pour certains pays selon leur contexte



Modèles Hybrides

Pour ceux qui cherchent l'équilibre



Sans Identifiant Unique

Pas un retard mais un choix souverain

Le NIU n'est pas la solution miracle et idéale | **L'absence de NIU n'est pas un retard technologique**

CONCLUSION

Vers une décision souveraine et éclairée

- Le NIU est un outil puissant — mais tout outil puissant exige maîtrise technique, vigilance juridique et éthique institutionnelle forte.
- Notre mission : favoriser une prise de décision éclairée et souveraine, plutôt qu'un alignement idéologique.
- L'Afrique peut inventer ses propres modèles, adaptés à ses réalités.

« Quel système est le plus juste pour nos citoyens ? »

Merci de votre aimable attention

M. Adamou IRO

Président — HAPDP Niger | Président — NADPA/RAPDP | Ambassadeur adjoint ID4Africa

ID4Africa 2026