



# Sécurisation des systèmes nationaux d'identité en RD Congo

Une approche stratégique de souveraineté et de confiance numérique

**Monsieur Aimé MUKUMA**

Conseiller DPI & Cybersécurité

Agence pour le Développement du Numérique



# Une vision portée au plus haut sommet de l'État



*« La sécurité et la souveraineté numériques sont une responsabilité essentielle de l'État : protéger nos systèmes de communication et nos infrastructures critiques face aux cybermenaces, aux vulnérabilités des données et à la dépendance technologique. »*

— **Son Excellence Félix-Antoine TSHISEKEDI TSHILOMBO**

*Président de la République Démocratique du Congo*

# La RDC en chiffres : un géant numérique en construction

**110**

MILLIONS

*de Congolais à identifier*



**69,4 M**

**abonnés mobiles actifs**

*ARPTC, T2 2025 — +9 % en un an*



**34,5 M**

**abonnés Internet mobile**

*Taux de pénétration ≈ 31 %*



**44 M**

**fichier CENI transmis à l'ONIP**

*Base biométrique mutualisée*



**60 %**

**de la population a < 20 ans**

*Pression sur l'enrôlement futur*



**33 + 1**

**FAI agréés (dont Starlink)**

*Surface d'attaque démultipliée*



**10 ans**

**validité de la CIN biométrique**

*Décret n° 22/08 du 2 mars 2022*

# L'identité numérique : une infrastructure stratégique

*Sécuriser l'identité numérique, c'est sécuriser le pacte entre l'État et le citoyen.*

*L'identité numérique touche aujourd'hui à quatre dimensions vitales :*



## **Sécurité nationale**

Protection des frontières, lutte contre la criminalité, antiterrorisme.



## **Gouvernance publique**

Fiabilité des registres, transparence et continuité de l'action publique.



## **Inclusion sociale**

Accès aux droits, aux services essentiels, à la citoyenneté pleine.



## **Stabilité économique & démocratique**

Confiance des opérateurs, intégrité électorale, attractivité du pays.

# Les nouveaux risques des systèmes d'identité



## Cyberattaques

Attaques ciblées contre les bases de données nationales, ransomware, exfiltration massive.



## Fraude & usurpation

Création de fausses identités, vol d'identifiants biométriques, contournement des contrôles.



## Dépendance technologique

Souveraineté des données menacée par des choix d'architecture et de fournisseurs non maîtrisés.



## Infrastructures critiques

Vulnérabilités physiques et logiques sur les centres de données, réseaux et points d'enrôlement.



## Données personnelles

Défi de protection à grande échelle : volumétrie, sensibilité, cycle de vie, transferts.

# L'écosystème institutionnel du numérique en RDC



PRÉSIDENTENCE DE LA RÉPUBLIQUE

Vision · Arbitrage · Coordination  
stratégique



PT

Ministère des Postes et Télécommunications



ÉCO. NUM.

Ministère de l'Économie Numérique



INTÉRIEUR

Ministère de l'Intérieur & Sécurité

ARPTC

Régulateur télécoms

ONIP

Identification  
population

ADN

Agence pour le  
Développement du  
numérique

CNC

Conseil National de  
Cyberdéfense

CNN\*

Conseil National du  
Numérique

En cours de création

ANCY\*

Agence Nationale de  
Cybersécurité

En cours de création

# L'approche stratégique de la RDC



## VISION

**Faire de l'identité numérique un pilier de la souveraineté et de la confiance.**

*Une stratégie articulée autour de cinq leviers structurants.*



### **Intégration progressive du Cyber**

Inclusion systématique des enjeux de cybersécurité dans tous les projets numériques nationaux.



### **Gouvernance et coordination**

Renforcement des mécanismes interinstitutionnels : pilotage clair, responsabilités définies, coordination opérationnelle.



### **Vision de résilience nationale**

Référentiels de sécurité, gestion des risques, exercices de crise, capacités de réponse à incident.



### **Security by design**

La sécurité n'est plus une couche ajoutée : elle est intégrée dès la conception des systèmes d'identité.



### **Souveraineté juridique**

Convention de Malabo, Réseau national des DPO, Autorité de protection des données personnelles.

# Le défi africain : sécuriser sans reproduire les dépendances



**Un impératif continental**



## Développement de capacités locales

Formation, talents, écoles de cybersécurité, écosystèmes universitaires et industriels nationaux.



## Partenariats équilibrés

Coopérer avec les acteurs internationaux sans aliéner la décision, la donnée et le savoir-faire.



## Interopérabilité & gouvernance

Standards ouverts, gouvernance partagée, mécanismes africains de confiance entre États.



## Solutions

Architectures adaptées aux contraintes locales : connectivité, énergie, langues, capacités, ressources.

# Vers une identité numérique résiliente et souveraine

*La cybersécurité doit être pensée dès la conception des systèmes d'identité et la confiance numérique deviendra un pilier majeur de la stabilité des États.*

1

**Sécurisé**

Protégé contre les menaces actuelles et futures.

2

**Résilient**

Capable d'absorber les chocs et de continuer à fonctionner.

3

**Inclusif**

Au service de tous les citoyens, sans exclusion.

4

**Respectueux des citoyens**

Données personnelles protégées, droits garantis.

5

**Aligné sur la souveraineté**

Articulé avec la souveraineté numérique africaine.



MOT DE CLÔTURE

***La RDC construit actuellement les fondations d'un écosystème d'identité numérique résilient, souverain et sécurisé, en intégrant dès aujourd'hui les enjeux de cybersécurité, de gouvernance et de confiance numérique.***



**Merci**