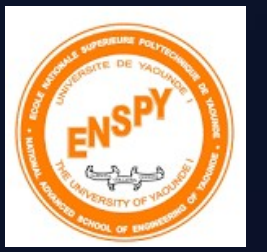
WORK-GMC 2026

Protéger le cyberespace Camerounais de demain

Bâtir la confiance numérique à l'ère post-quantique

Hervé TALE KALACHI

DÉPARTEMENT DE GÉNIE INFORMATIQUE
ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE DE YAOUNDÉ (ENSPY)



La mécanique de la transformation

Services

Mise en ligne des infrastructures

Confiance

Sécurité et garantie de l'État

Usage

Adoption massive par les citoyens

Transformation

Développement de l'économie numérique

L'Équation du Numérique

Services en ligne

Digitalisation des processus métier

Confiance Numérique

Condition sine qua non de l'adoption

Usage Massif

Catalyseur de l'économie nationale

"Sans confiance, pas d'usage. Sans usage, pas de transformation."

Le déficit de confiance technique

90%

Paiements à la livraison

vs 10% en e-paiement (Jumia Cameroun)

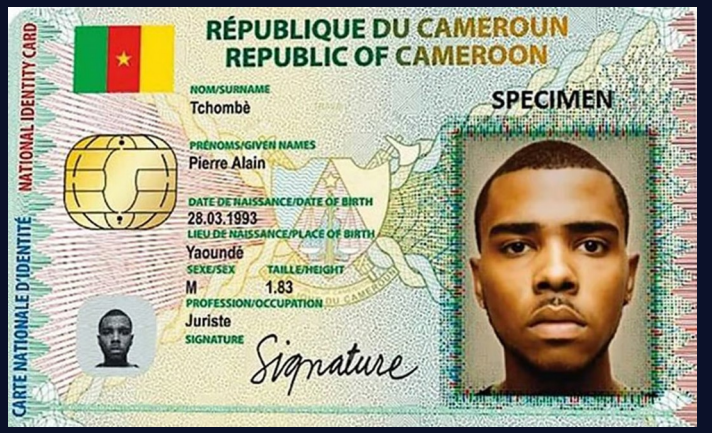
L'obstacle n'est pas technologique, il est psychologique.

L'ANTIC révèle que les audits de sécurité sur nos fintechs en 2025 montrent encore des vulnérabilités (faux SMS, liens frauduleux).

Sans une sécurisation robuste, le citoyen préfère le cash.

Sources: World Bank (Digital Economy Assessment) / ANTIC (Audits 2025)

L'identité, fondation du service



L'absence de preuve d'identité est le frein numéro 1.

36 % des adultes non bancarisés citent ce manque comme obstacle principal à l'inclusion financière.

La confiance numérique nécessite d'abord de savoir "qui" se connecte.

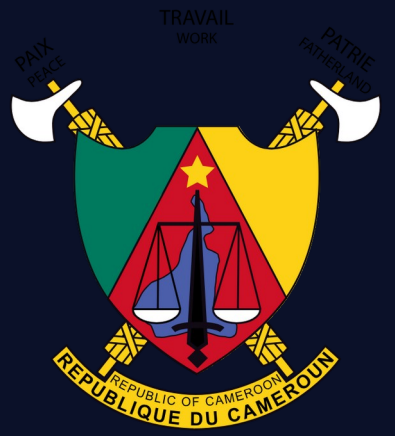
7,5M

de Camerounais

sans preuve officielle d'identité

Source: World Bank (Identity Ecosystem Analysis in Cameroon 2023)

La crédibilité de l'État attaquée



987

Faux comptes détectés

en 2023

843

Comptes neutralisés

Protéger l'authenticité

L'usurpation d'identité institutionnelle détruit la confiance citoyenne.

- 86 comptes certifiés depuis 2018
- Déploiement du DNSSEC sur le '.cm'

Source: ANTIC 2024 (Veille sécuritaire)

Plan de l'exposé

01 **Piliers & Cadre Réglementaire Actuel**

02 **La Menace Quantique**

03 **Migration & Standards NIST**

01

Piliers & Cadre Réglementaire

L'architecture de la Confiance

- **Identité & Authentification :** S'assurer que chaque acteur est bien celui qu'il prétend être.
- **Confidentialité & Données :** Protéger les échanges et la vie privée des citoyens.
- **Intégrité & Non-répudiation :** Garantir qu'aucune transaction ne peut être altérée ou reniée.
- **Disponibilité & Résilience :** Assurer un service continu face aux attaques.
- **Gouvernance & Audit :** Contrôler, sanctionner et adapter le cadre en permanence.

Le Cameroun ne part pas de zéro

2010

Lois sur la Cybersécurité, Com. Électroniques & E-commerce

L'ANTIC

Régulation, veille sécuritaire et certification électronique

CIRT

Centre national de réponse aux incidents de cybersécurité

Déc. 2024

Loi (2024/017) sur la protection des données personnelles

Sources: Lois 2010/012, 013, 021, 2024/017 / ANTIC (Textes organiques)

02
La Menace Quantique

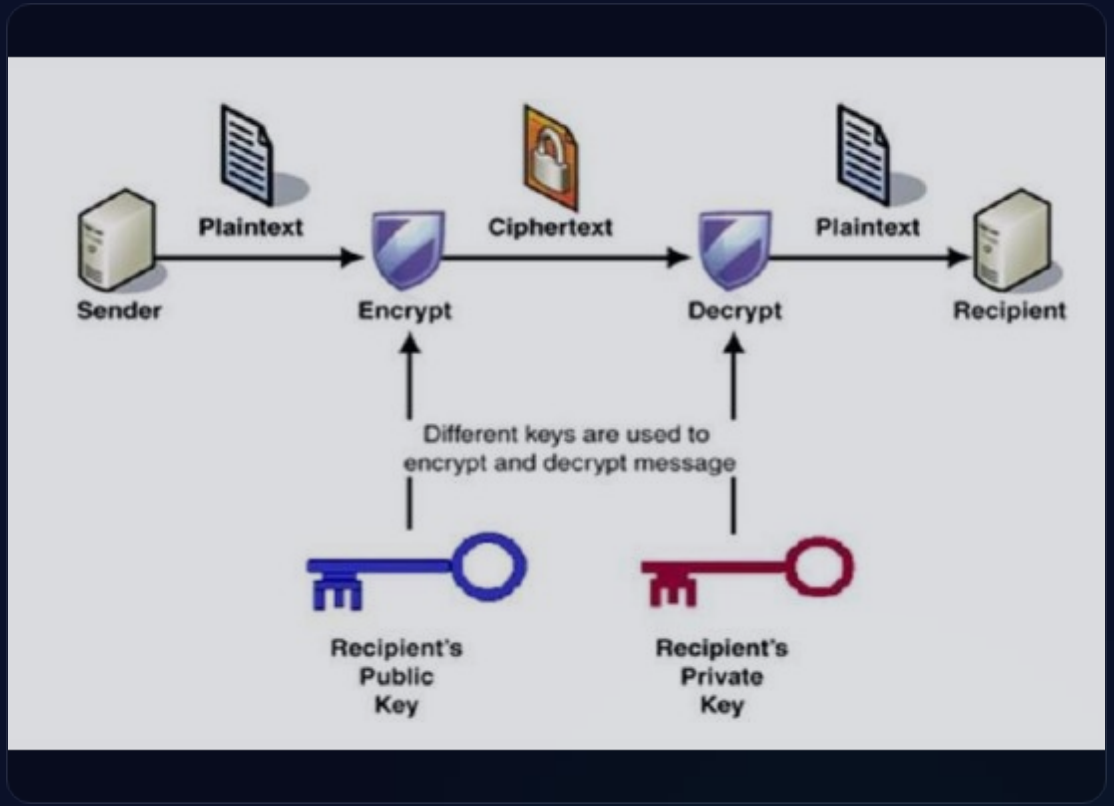
Sous le capot : le socle invisible

La Cryptographie à Clé Publique

Toute l'architecture de confiance repose sur des fondations mathématiques.

- L'établissement des clés (Diffie-Hellman)
- Les certificats TLS
- Les signatures électroniques (RSA, ECDSA)
- L'authenticité des acteurs

Sans ce socle asymétrique, Internet s'effondre.



1994 : La Menace Algorithmique Quantique

L'Algorithme de Peter Shor

Un ordinateur quantique peut briser la factorisation et le logarithme discret.

$$f(x) = a^x \bmod N$$

$$N = p \times q$$

1994 : La Menace Algorithmique Quantique

Impact : RSA, DH et ECDH deviennent instantanément obsolètes dès l'apparition d'un processeur quantique à large échelle.

La menace algorithmique n'est plus une hypothèse.

Source: Peter Shor, 1994, Algorithms for Quantum Computation

La menace est déjà stratégique

"Harvest Now, Decrypt Later"

1. Intercepter (Aujourd'hui)

Capturer les flux de données chiffrés (secrets d'état, identités, transactions) qui transitent sur les réseaux.

2. Stocker

Conserver ces données massives dans des data centers en attendant l'avènement matériel de la technologie quantique.

3. Déchiffrer (Demain)

Briser le chiffrement rétroactivement. Une menace mortelle pour les données à longue durée de vie.

Source: CISA/NSA/NIST Quantum Readiness factsheet

03
Migration & Standards NIST

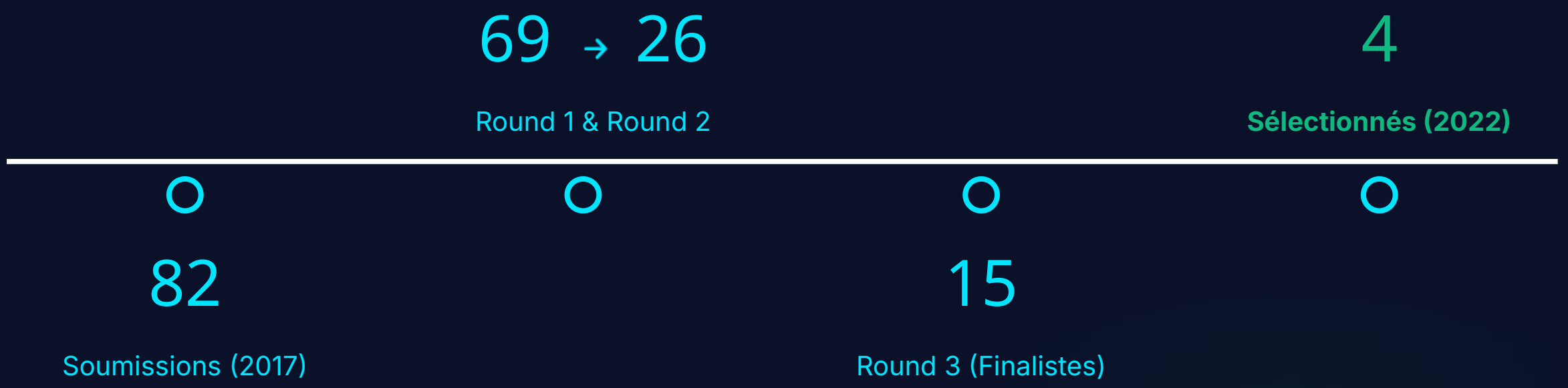
La réponse mondiale (2016)

L'initiative Post-Quantique du NIST

Face à une menace vitale pour l'économie numérique, la réponse ne pouvait être improvisée.
Le NIST a initié un effort de standardisation mondial, ouvert, exigeant et rigoureux, mobilisant toute les communautés Crypto de la planète.

Source: NIST Post-Quantum Cryptography project page

La sélection la plus « rigoureuse » de l'histoire



Sources: NIST Status Reports on Rounds 1, 2, 3 / 2022 announcement

L'ère opérationnelle a commencé

Standards FIPS (Août 2024)

La cryptographie post-quantique n'est plus de la recherche théorique.

FIPS 203 : Échange de clés (ML-KEM)

FIPS 204 : Signatures (ML-DSA)

FIPS 205 : Signatures (SLH-DSA)

Nouveaux ajouts (2025)

La diversification des algorithmes se poursuit pour garantir la robustesse.

HQC : Sélectionné pour standardisation (2025).

Falcon : Processus de standardisation toujours en cours.

Sources: NIST (Approval of FIPS 2024, selection of HQC 2025)

L'enjeu pour le Cameroun

Ne pas paniquer. Anticiper.

La normalisation internationale dicte désormais le tempo de l'industrie technologique mondiale.
Le sujet pour le Cameroun n'est pas de débrancher toutes nos infrastructures demain matin.

L'enjeu est de cartographier, tester et gouverner la migration de notre souveraineté numérique.

Source: NIST IR 8547 on transition to PQC standards

Exemple de Feuille de route stratégique

- **Inventaire cryptographique :** Identifier systématiquement où RSA et ECC sont utilisés dans nos systèmes étatiques.
- **Priorisation par le risque :** Traiter en urgence les données sensibles à longue durée de vie.
- **Crypto-agilité :** Imposer la flexibilité algorithmique dans les futurs cahiers des charges.
- **Pilotes et interopérabilité :** Lancer des tests locaux sur des infrastructures non critiques.
- **Gouvernance nationale :** Coordonner la préparation post-quantique au plus haut niveau.

Source: NIST / NCCoE Migration to Post-Quantum Cryptography

Souveraineté et Compétences

Le rôle de la recherche camerounaise

Former des compétences locales est le seul moyen de garantir notre indépendance technologique.

- Appuyer la décision publique par une expertise locale.
- Travaux académiques locaux sur la *Security and privacy in data governance*.
- Travaux en cours sur la migration vers PQC dans les protocoles de sécurité.

La loi est une boussole.
L'action est le chemin.

Le cadre réglementaire camerounais (2010 - 2024) est solide et essentiel.

Cependant, un texte juridique seul n'arrête pas une cyberattaque.

L'application effective, le contrôle, l'audit technique et l'anticipation des ruptures comme le quantique sont nos véritables boucliers.

"Protéger le cyberespace camerounais de demain, c'est faire en sorte que la confiance numérique d'aujourd'hui devienne une capacité nationale durable."

WORK-GMC 2026