

Enjeux de la Confiance Numérique pour les pays africains

SG 13 RG- AFR

Session 5 : Trust and Technology Convergence

William KADIO
Chef de Service
Dématisation
ARTCI

SOMMAIRE

- **CONTEXTE – DEVELOPPEMENT DE L'USAGE DES TICS EN AFRIQUE**
- **RISQUES DE SECURITE**
- **CONFIANCE NUMERIQUE**
- **ENJEUX DE LA CONFIANCE NUMERIQUE**
- **AUTORITES, PRESTATAIRES ET INFRASTRUCTURES DE CONFIANCE NUMERIQUE**
- **RECOMMANDATIONS**

CONTEXTE

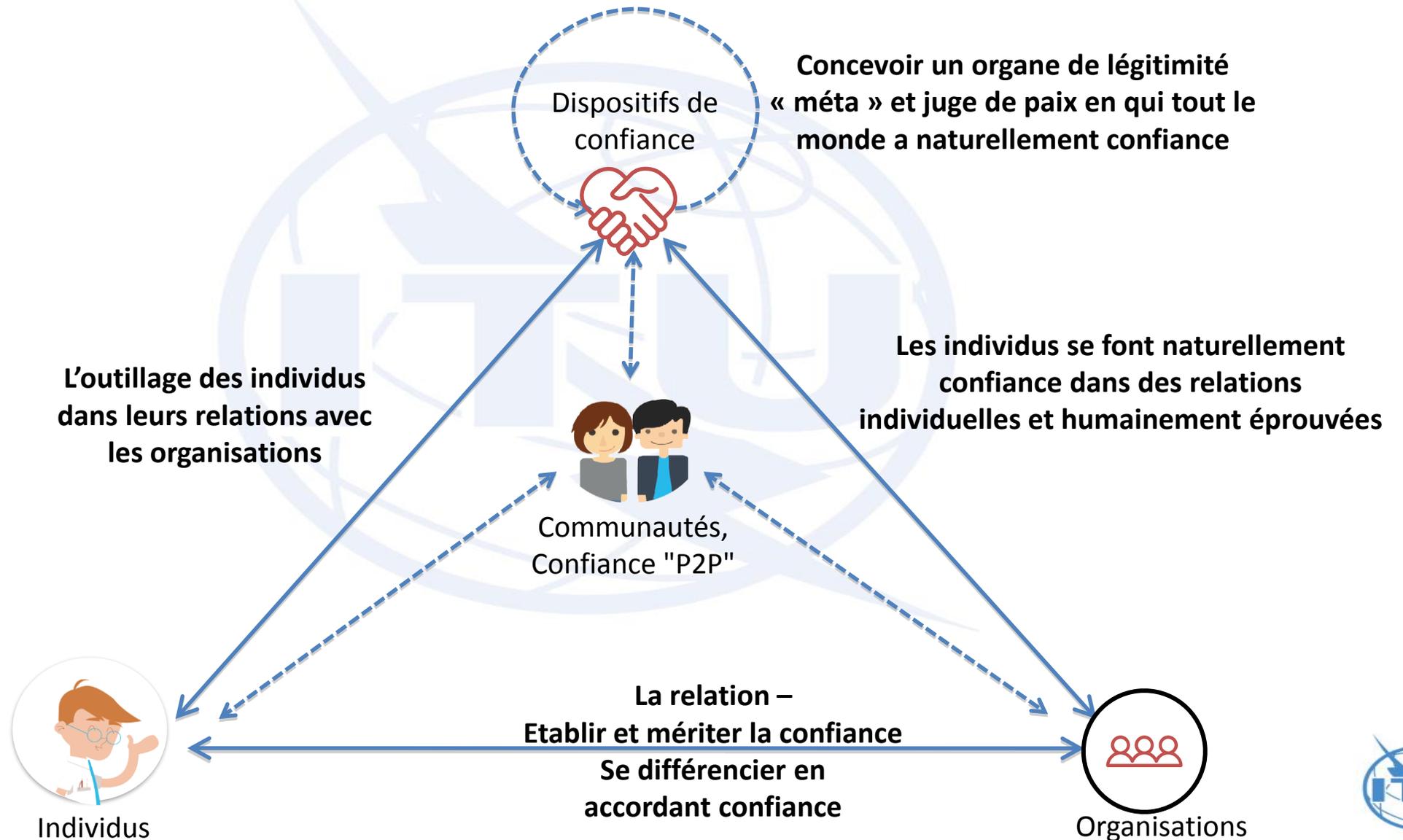
- **Nouvelles technologies et leurs usages**
 - 3G, 4G, 5G, IoT, Cloud Computing, Smart Grid, Smart City...
 - Commerce Electronique, E-gouvernance, m-Gouvernance, e-agriculture, m-agriculture, Services Financiers Mobiles, réseaux sociaux, e-education...
- **Impacts économiques et sociaux**
 - Accroissement échanges électroniques entre les citoyens et les gouvernements (e-voting...)
 - Facteur de développement économique (8% PIB en CI)
 - Inclusion financière (SFM), Banque rurale mobile
 - Développement de la sphère entrepreneurial autour des Tics, réduction du chômage
 - Accroissement de la cybercriminalité

RISQUES DE SECURITE

- **Cybercriminalité**
 - Arnaque au sentiment, cyber-chantage
 - Usurpation d'identité
 - harponnage (phishing)
 - Rançongiciel (Ransomware)
- **Perte de la vie privée**
 - Usage abusif des données personnelles
 - Divulgation des données personnelles
- **Perte de la Sécurité de l'information**
 - Perte de la confidentialité des informations
 - Destruction des informations
 - Interruption des services (DDoS)
- **Protection en ligne des enfants**
 - Contact avec des inconnus
 - Usages excessifs des TICS (dépendance des jeux en ligne), absence de contrôle parental
 - Images violentes, Racistes, pornographiques...

La confiance des usagers dans les technologies repose aujourd'hui sur un équilibre fragile : plus les usages numériques se démocratisent et s'étendent, plus la confiance des utilisateurs peut s'éroder

CONFIANCE NUMERIQUE - OVERVIEW



CONCEPTS AUTOURS DE LA CONFIANCE NUMERIQUES

- Cadre juridique
- Autorité régaliennne d'agrément et de contrôle
- Normes et politiques
- Identité numérique
- Utilisation de services de confiance (certification électronique, signature électronique, authentification, confidentialité des données, conservation – archivage des données)
- Prestataires de services (ou tiers) de confiance

ENJEUX DE LA CONFIANCE NUMERIQUE

- Mettre en place un cadre juridique et une autorité nationale de confiance (droits, devoirs et sanctions)
- Instaurer la confiance dans les prestataires de services
- S'assurer de la maîtrise des risques de sécurité liés à l'usage des nouvelles technologies
- Veiller à la Protection des usagers ou consommateurs
- Veiller à la Protection des données à caractère personnel

ENJEUX DE LA CONFIANCE NUMERIQUE

- Sensibiliser les différents acteurs
- Protéger les systèmes d'informations et réseaux des organisations (plus particulièrement des infrastructures critiques)
- Promouvoir et utiliser les standards internationaux dans le domaine de la sécurité de l'information
- Offrir aux usagers un accès transparent, permanent et sécurisé aux services
- Veiller à la protection en ligne des enfants

AUTORITES DE CONFIANCE NUMERIQUE

Les **Autorités de Confiance** sont chargées de mettre en place un cadre réglementaire pour la confiance numérique (Politiques, standards, règles de contrôle...)

- ❖ Agrément/ Autorisation et Contrôle des prestataires de services de confiance
 - ❖ Etablissement de politiques et standards
 - ❖ Promotion de la confiance numérique
-
- **Autorité Nationale de Sécurité des Systèmes d'Information**
 - **Autorité Nationale pour la Protection des Données Personnelles**
 - **Autorité Nationale pour la Certification Electronique**

PRESTATAIRES DE SERVICES CONFIANCE NUMERIQUE

- **PSCE**
 - Prestataire de services de certification électronique, chargé de délivrer les certificats électroniques (identités numériques) et de fournir des services en matière de signature électronique
- **PASSI**
 - Prestataire d'Audit de Sécurité des Systèmes d'Informations, chargé de veiller à la sécurité et à l'audit de sécurité des systèmes d'informations et réseaux
- **PSAE**
 - Prestataire des services d'archivage électronique, chargé d'assurer la dématérialisation et la conservation des archivages électroniques
- **CERTs**
 - Centres techniques chargés de détecter et de répondre aux incidents et de protéger le cyberspace national contre les attaques informatiques de grandes ampleurs

INFRASTRUCTURES DE CONFIANCE NUMERIQUE

- **SOC (Security Operation Center)**
 - S'assurer de la détection et de la réponse aux incidents au sein du cyberspace nationale
- **PKI (WEB Public Key Infrastructure)**
 - S'assurer de la délivrance et gestion des identités numériques pour les personnes physiques, morales (entreprises) et les machines (serveurs ou objets connectés)
 - Authentification, signature électronique et chiffrement
- **RPKI (Ressources Public Key Infrastructure)**
 - Améliorer la sécurité du système de routage de l'Internet, en particulier le protocole de passerelle frontière (BGP).
 - Sécuriser l'assignation autorisée des ressources IP et numéro AS aux registres Internet locaux (LIR)
- **DNSSEC (DNS Security Extensions)**
 - pour authentifier l'information sur le DNS par la signature numérique des enregistrements DNS
 - Protéger le DNS contre toute pollution intentionnel
 - garantir qu'un serveur de nom ne fournit pas des informations fausses pour diriger les utilisateurs vers des hôtes qui contrôlent leurs transactions ou se font passer pour d'autres sites.

RECOMMANDATIONS

- Mise en place du Cadre juridique et réglementaire pour la sécurité des transactions électroniques et des systèmes d'informations (cybercriminalité, cybersécurité, protection des données personnelles...)
- Mise en place des Autorités Nationales, de Protection des Données Personnelles, de Certification Electronique et de Sécurité des Systèmes d'Information
- Sensibilisation des usagers sur les risques de sécurité liés aux usages des technologies de l'information
- Mise en place d'infrastructure de Confiance Numérique
- Mise en place de plateforme pour la Protection en ligne des enfants



MERCI !!!!!!!