Note conceptuelle : *Atelier régional sur la cartographie des infrastructures de fibre optique pour stimuler l'investissement et accélérer la connectivité universelle en Afrique centrale.*

1. Contexte et introduction :

En Afrique centrale, la fracture numérique reste l'une des plus marquées du continent. Malgré les progrès réalisés dans certains pays, l'accès au haut débit demeure limité, coûteux et inégalement réparti. Si les grandes villes bénéficient d'une couverture relativement satisfaisante, les zones rurales et transfrontalières restent largement sous-desservies, privant des millions de personnes d'un accès régulier et fiable à Internet. Cette situation freine la compétitivité économique et accentue les inégalités sociales et territoriales.

Un défi majeur tient à l'absence de données précises, fiables et régulièrement mises à jour sur la couverture réelle des réseaux. La plupart des statistiques disponibles reposent sur les déclarations des opérateurs, sans vérification indépendante ni niveau de détail suffisant. Or, des informations fiables sont indispensables pour planifier des politiques publiques efficaces, orienter les investissements et mettre en œuvre des actions ciblées de réduction de la fracture numérique.

Pour répondre à ce besoin, l'ARTAC, en partenariat avec l'UIT, propose de mettre en œuvre un projet de cartographie du haut débit en Afrique centrale. L'atelier présentera la méthodologie permettant de mesurer les lacunes dans l'infrastructure des TIC et de planifier les activités de connectivité. Il vise à renforcer les compétences théoriques et pratiques des participants dans la collecte de données sur l'infrastructure des TIC, l'identification des zones mal desservies, l'application d'outils SIG et l'utilisation de modèles de connectivité pour tester et comparer des scénarios de connectivité sélectionnés.

Au cours de sessions pratiques, les participants échangeront leurs expériences respectives tout en étant formés à l'identification et la préparation de leurs propres données à l'aide de dictionnaires de données et de normes courantes. Les sessions couvriront des sujets tels que l'analyse exploratoire des données, la validation des données, la visualisation et des sujets plus avancés tels que l'analyse de la visibilité pour la connectivité point à point et l'analyse du chemin de la fibre.

L'atelier fournira des informations sur la façon d'utiliser la plateforme de planification de la connectivité (CPP), un nouvel outil axé sur les données qui aide les gouvernements, les régulateurs, les opérateurs et les partenaires à prendre des décisions fondées sur des données probantes grâce à des données intégrées, une modélisation dynamique et des informations exploitables pour la planification du haut débit et du dernier kilomètre (notion qui fait référence à l'installation finale du câble de fibre jusqu'au domicile ou lieu de travail de l'abonné, représentant la section la plus complexe et coûteuse du réseau)

De plus, dans le cadre de la collaboration entre l'UIT et l'ARTAC en 2025 sur les données et la cartographie des infrastructures, les résultats de la recherche documentaire menée dans les 8 États membres de l'ARTAC (Burundi, Cameroun, Gabon, Congo, République démocratique du Congo, République centrafricaine, Guinée équatoriale, Tchad) seront partagés et discutés.

2. Objectif général

L'objectif principal de cet atelier est de renforcer les capacités des pays d'Afrique centrale à concevoir et déployer un système de cartographie du haut débit fiable, interactif et régulièrement actualisé, afin de favoriser une meilleure transparence, une planification plus efficace des infrastructures numériques et, in fine, de promouvoir l'inclusion digitale et le développement durable :

- Collecter, centraliser et harmoniser l'ensemble des données existantes relatives à la couverture haut débit.
- Renseigner la plateforme cartographique interactive, accessible aux décideurs publics, aux opérateurs de télécommunications et aux citoyens.
- Identifier et cartographier de manière précise les zones non desservies ou mal desservies, en vue de prioriser les besoins d'investissement.
- Renforcer la transparence, la concertation et la collaboration entre les parties prenantes du secteur numérique.
- Mettre en place un mécanisme de mise à jour régulière et participative des données

3. Agenda

15 décembre 2025	Introduction et principes fondamentaux de l'analyse géospatiale avec discussions autour des données existantes dans les Etats membres de l'ARTAC
08 :30-09 :00	Enregistrement
09 :00-09 :30	Allocation Tchad. Allocution UIT Allocution ARTAC
09 :30-09 :45	Photo de famille
09 :45-10 :30	Introduction et contexte de la collaboration UIT-ARTAC
10 :30-11 :00	Pause-café
11 :00-12 :30	Planification des activités de déploiement des infrastructures TIC Types de données géospatiales, projections et systèmes de coordonnées
12 :30-13 :30	Pause déjeuner
13 :30-15 :15	Standardisation des données Analyse de proximité et analyse de couverture
15 :15-15 :30	Pause-café
15 :30-17 :00	Télécommunications, données ouvertes et collecte de données ouvertes Discussion et partage sur les données d'infrastructure, résultats de la recherche documentaire dans les États membres de l'ARTAC

16 décembre 2025	Applications avancées et planification d'entreprise
09 :00-10 :30	Analyse de la demande, analyse de la visibilité, analyse des chemins de fibre et analyse des coûts pour concevoir des réseaux de fibre efficaces en exploitant l'infrastructure existante et en optimisant les tronçons pour en assurer la rentabilité
10 :30-11 :00	Pause-café
11 :00-12 :30	Vue d'ensemble des outils existants et de leurs applications, y compris les outils de visualisation open source
12 :30-13 :30	Pause déjeuner
13 :30-15 :15	Aperçu et facilité d'utilisation de la plate-forme de planification de la connectivité (CPP) pour les États membres de l'ARTAC
15 :15-15 :30	Pause-café
15 :30-16 :30	Echanges et partages de vues sur les prochaines étapes

4. Exigences techniques de formation

Exigences du lieu pour la formation pratique (hors ligne) :

- Un laboratoire informatique avec un accès Internet et un projecteur.
- Microphones et système audio (haut-parleurs).
- Connexion Internet stable et ininterrompue pour tous les participants.
- *Possibilité pour les participants hors ligne de se connecter à Internet à l'aide de leurs appareils portables (ordinateurs portables et smartphones).*
- *Possibilité pour les participants en ligne de suivre la formation.*
- Possibilité pour les intervenants en ligne d'animer la formation pendant leurs sessions.

Exigences logicielles et matérielles pour la pratique de la cartographie et de l'analyse SIG :

Logiciel :

- **QGIS version 3.34.11 'Prizren LTR'** (version à long terme) : Pour les systèmes d'exploitation Windows, Mac et Linux
- Logiciel pour lire et modifier des fichiers .xls, .xlsx .csv (par exemple, MS Excel).
- Logiciels de **navigation sur le Web** : Chrome, Firefox ou Safari

Matériel :

- RAM - 8 Go de RAM ou plus sont recommandés pour utiliser QGIS et éviter les pannes du système.
- La vitesse du processeur -1,8 GHz est recommandée, mais pas obligatoire. QGIS peut fonctionner lentement à des niveaux inférieurs.
- Stockage sur disque dur - Cela dépend des ensembles de données, 1 Go suffirait dans la plupart des cas.

Comptes et informations d'identification :

Les utilisateurs devront disposer d'un compte Google fonctionnel (personnel ou professionnel) pour exécuter les blocs-notes Google Colab. Vous trouverez ici des instructions https://support.google.com/accounts/answer/27441?hl=en sur la création d'un compte Google.

Note Conceptuelle : *Clinique des services financiers numériques (SFN)*

Contexte et introduction :

La croissance des services financiers numériques (SFN) à travers l'Afrique a transformé la façon dont les gens accèdent et utilisent les produits financiers, accélérant l'inclusion financière et permettant de nouvelles formes d'innovation. Cependant, cette expansion rapide a également exposé les utilisateurs, les fournisseurs et les régulateurs à un éventail croissant de risques de sécurité, allant des **vulnérabilités de signalisation (par exemple, SS7)** et de **la fraude par échange de cartes SIM** aux **menaces au niveau des applications** et **aux défis de cyberrésilience** dans les infrastructures critiques.

Pour résoudre ces problèmes, l'Union **internationale des télécommunications (UIT)** a élaboré les recommandations de sécurité DFS et a créé le laboratoire de **sécurité SFN** en 2020. Le laboratoire fournit aux organismes de réglementation et aux fournisseurs de services des outils pratiques, une formation ciblée et des conseils techniques pour renforcer la confiance dans l'écosystème des SFN. Par l'intermédiaire du laboratoire de sécurité SFN, l'UIT fournit une assistance technique aux régulateurs des économies émergentes pour mettre en place leurs laboratoires de sécurité SFN et adopter les Recommandations de sécurité SFN.

Les recommandations de sécurité SFN ont été adoptées en tant que normes internationales par la Commission d'études 17 de l'UIT-T sous les noms **ITU-T X.1277.2 (04/2023) : Cadre de sécurité pour les services financiers numériques** et **UIT-T X.1456 : Lignes directrices pour la sécurité des services financiers numériques.**

Les cliniques de sécurité sont des **ateliers pratiques de renforcement des capacités** qui rassemblent des régulateurs, des opérateurs de réseaux mobiles, des fournisseurs de services financiers et des décideurs politiques afin d'évaluer et de renforcer la sécurité des écosystèmes SFN. Chaque clinique présente aux participants la méthodologie et les outils du Laboratoire de sécurité SFN de l'UIT, ce qui leur permet de :

- Effectuer des évaluations pratiques de la sécurité des applications et des infrastructures DFS (par exemple, USSD, STK, Android, iOS).
- Identifiez et atténuez les vulnérabilités systémiques, telles que les défauts de signalisation SS7, l'échange/le recyclage de la carte SIM et les faiblesses des applications mobiles.
- Appliquer des cadres d'assurance de la sécurité et des listes de contrôle de conformité alignés sur les Recommandations de **sécurité SFN de l'UIT.**
- Renforcez la cyberrésilience grâce à de meilleures mesures de détection, d'intervention et de récupération des incidents.
- Élaborer des programmes de sensibilisation et d'alphabétisation des consommateurs afin de renforcer la confiance du public dans les services financiers et aux services numériques.
- Collaborer entre les secteurs pour élaborer des feuilles de route d'action nationales et régionales pour la sécurité des SFN.

Les participants repartent avec des outils pratiques et les prochaines étapes concrètes pour intégrer les contrôles de sécurité des SFN dans la réglementation, la surveillance et la prestation de services.

L'UIT organisera une **clinique de sécurité pour la région de l'ARTAC**. Cet événement servira de **point d'entrée pour que les pays de l'ARTAC commencent à adopter les Recommandations de sécurité SFN de l'UIT au niveau régional**. Ces recommandations, notamment **UIT-T X.1277.2 (04/2023) : Cadre de sécurité pour les services financiers numériques et UIT-T X.1456 : Lignes directrices en matière de sécurité pour les services financiers numériques**, fournissent un ensemble structuré de contrôles et d'attentes prudentielles visant à atténuer les risques dans l'ensemble des écosystèmes de SFN.

Résumé des directives et recommandations de sécurité SFN

1. Recommandations à l'intention des régulateurs pour atténuer les vulnérabilités SS7 : détails sur les recommandations à l'intention des régulateurs de la SFN et des opérateurs de réseaux mobiles pour atténuer les effets des vulnérabilités SS7.

2. Recommandations de sécurité pour se protéger contre les risques de SFN sur les cartes SIM et la fraude par échange de cartes SIM : - conseils et recommandations pour les régulateurs et les fournisseurs afin d'atténuer les vulnérabilités des cartes SIM telles que les échanges de cartes SIM, le recyclage des cartes SIM et les attaques sur les cartes SIM telles que les attaques binaires en direct.

3. Meilleures pratiques en matière de sécurité des applications mobiles : les meilleures pratiques en matière de sécurité des applications de services financiers mobiles que les régulateurs de la SFN peuvent adopter à titre de lignes directrices.

4. Modèle de protocole d'entente type entre un organisme de réglementation des télécommunications et une banque centrale sur la sécurité des services financiers numériques : - comprend des clauses qui traitent de la sécurité des SFN que les régulateurs devraient envisager d'adopter ou d'intégrer dans les protocoles d'entente existants.

5. Cadre de compétences des consommateurs de SFN : Le cadre de compétences des consommateurs DFS fournit des conseils aux décideurs politiques, aux régulateurs nationaux et aux fournisseurs de SFN lors de l'élaboration de programmes de sensibilisation et d'alphabétisation des consommateurs dans le cadre de la stratégie SFN/inclusion financière.

Il est important de noter que ces recommandations ont déjà été **adoptées par l'Association des régulateurs des communications d'Afrique australe (CRASA)** et l'**Organisation des communications de l'Afrique de l'Est (EACO),** et sont **à l'étude pour adoption par l'Assemblée des régulateurs des télécommunications d'Afrique de l'Ouest (ATRAO).** La Clinique de Sécurité ARTAC représente donc une opportunité charnière pour étendre cette dynamique à l'Afrique centrale.

Description de la Clinique de Sécurité

La clinique va :

- Proposer **des sessions approfondies** sur les vulnérabilités de SFN courantes, notamment SS7 et les défauts de signalisation, l'échange et le recyclage de la carte SIM, ainsi que les faiblesses de la sécurité des applications.
- Mettre en place **des cadres d'assurance de la sécurité** pour aider les organismes de réglementation et les fournisseurs à surveiller la conformité aux contrôles de sécurité minimaux.
- **Présenter les outils et la méthodologie du laboratoire de sécurité de SFN**, y compris la manière dont les régulateurs et les fournisseurs peuvent effectuer des évaluations de sécurité pratiques des applications de SFN exécutées sur USSD, STK, Android, iOS pour évaluer la conformité aux recommandations de sécurité des SFN.
- Aborder la **cyberrésilience et la réponse aux incidents,** en aidant les pays à renforcer la préparation, la détection et le rétablissement en cas de cyberincidents liés aux SFN.
- Discuter **des implications politiques et réglementaires**, y compris la coopération inter institutions entre les organismes de réglementation des télécommunications, les banques centrales et les organismes de protection des consommateurs.
- Inclure des **stratégies de protection et de sensibilisation des consommateurs,** en dotant les décideurs politiques d'outils pour concevoir des programmes d'éducation et d'alphabétisation visant à renforcer la confiance du public.
- Guider les participants dans l'élaboration **de feuilles de route d'action au niveau national** en vue de l'adoption et de la mise en œuvre des Recommandations de sécurité de l'UIT sur la science-sédimentation, en vue d'une adoption régionale harmonisée dans le cadre de l'ARTAC.

Audience Cible

La clinique de sécurité de SFN réunira des régulateurs des télécommunications/TIC et des SFN, des opérateurs de réseaux mobiles, des fournisseurs de services financiers et d'autres parties prenantes des pays ARTAC dans le cadre d'un **programme interactif** conçu pour présenter, expliquer et opérationnaliser la mise en œuvre des Recommandations de sécurité de SFN de l'UIT

Résultats attendus

- **Introduction et familiarisation** des parties prenantes de l'ARTAC avec l'UIT-T X.1277.2 et l'UIT-T X.1456.
- **Lancement de l'adoption régionale** des recommandations de sécurité DFS au sein de l'ARTAC, complétant les adoptions déjà réalisées par la CRASA et l'EACO.
- **Amélioration de la sensibilisation et de la capacité technique** des organismes de réglementation, des opérateurs et des fournisseurs de services financiers numériques pour identifier et atténuer les risques de sécurité.
- **Renforcement de la collaboration** entre les pays de l'ARTAC en matière de surveillance, de supervision et d'échange d'information en matière de sécurité.
- Mise en place d'une **plateforme régionale d'échange de connaissances** pour soutenir la mise en œuvre continue et la coopération au-delà de la clinique.

Annexe A : Projet de programme de la clinique de sécurité de SFN

17 décembre 2025	Clinique de sécurité de SFN
08 :30-09 :00	**Séance d'ouverture** • Allocution de l'ARTAC • Allocution de l'UIT
09 :00-10 :15	**Introduction au laboratoire de sécurité de SFN de l'UIT et à la plate-forme de partage des connaissances** Cette séance donnera un aperçu général du laboratoire de SFN de l'UIT et de l'assistance qu'il fournit aux pays en développement pour l'adoption des recommandations relatives à la sécurité de SFN. Cette séance présentera également la plate-forme de partage des connaissances de l'UIT. La Plateforme de partage des connaissances en matière de sécurité des SFN de l'UIT est conçue pour favoriser la collaboration entre les régulateurs et les autres parties prenantes dans l'élaboration et la mise en œuvre de lignes directrices et de bonnes pratiques en matière de sécurité pour les services financiers numériques (SFN). Intervenant : Vijay Mauree, Venkatesen, ITU
10 :15-10 :30	Pause-café
10 :30-12 :30	**Recommandations de sécurité de SFN de l'UIT** – Partie 1 Cette séance mettra en évidence les mesures de sécurité à mettre en œuvre par les régulateurs et les fournisseurs de services numériques, comme mentionné dans les recommandations de sécurité de l'UIT pour sécuriser la couche applications, l'infrastructure de télécommunications et l'infrastructure du système de paiement. En particulier, les mesures suivantes seront présentées : • Recommandations de sécurité pour se protéger contre les risques de SFN liés aux cartes SIM et à la fraude par échange de cartes SIM • Modèle de protocole d'accord type entre un régulateur des télécommunications et une banque centrale sur la sécurité des services financiers numériques • Recommandations à l'intention des régulateurs pour atténuer les vulnérabilités SS7 • Cadre de compétences de SFN pour les consommateurs **Intervenant :** Vijay Mauree, Venkatesen, ITU
12 :30-13 :30	Pause déjeuner
13 :30-14 :45	**Recommandations de sécurité de SFN de l'UIT** – Partie 2 - Bonnes pratiques en matière de sécurité des applications Alors que les cybermenaces de SFN continuent d'évoluer, la protection des applications contre les vulnérabilités devient primordiale. Cette session explorera les tests de sécurité continus et l'intégration de la sécurité dans le cycle de vie du développement. Les régulateurs, les développeurs, les analystes de sécurité ou les responsables informatiques repartiront avec une compréhension de la mise en œuvre de mesures de sécurité robustes qui s'alignent sur les normes de l'industrie, garantissant ainsi la sécurité et l'intégrité des applications de SFN. **Intervenant :** Vijay Mauree, Venkatesen, ITU
14 :45-15 :00	Pause-café
15 :00-16 :00	**Cadre de cyberrésilience des SFN** Cette session présentera le kit d'outils de cyberrésilience de l'UIT pour les régulateurs afin de protéger les infrastructures financières numériques critiques. Cette séance comprendra également un exercice conçu comme une

	séance interactive sur table, où les participants ont été organisés en groupes, chacun se concentrant sur un aspect distinct de la cybersécurité : gestion des risques, gouvernance, essais, formation et sensibilisation, protection et réponse aux incidents. **Intervenant :** Vijay Mauree, Venkatesen, ITU
16 :00-17 :00	**Discussion ouverte : Adoption des recommandations de sécurité de SFN de l'UIT** Cette séance offrira un forum sur les prochaines étapes de l'adoption des recommandations de sécurité SFN par les membres de l'ARTAC.