ATTESTATION D'INTÉGRITÉ DE L'AFD

AMI N°_____

De :_____

Nous déclarons et nous nous engageons à ce que ni nous ni personne, y compris tout membre de notre joint-venture ou tout fournisseur, contractant, sous-traitant, consultant, sous-consultant, le cas échéant, agissant en notre nom avec l'autorité nécessaire ou avec notre connaissance ou consentement, ou facilité par nous, ne s'est engagé ou ne s'engagera dans une activité interdite en vertu de la Politique du Groupe AFD pour la prévention et la lutte contre les Pratiques Prohibées[1] dans le cadre de la présente procédure de passation de marché et (en cas d'attribution) de l'exécution du contrat susmentionné (« Contrat »), y compris tout amendement y afférent.

Nous acceptons de conserver tous les comptes, registres et autres documents (sur support papier ou électronique) relatifs à la passation et à l'exécution du contrat.

Nous, toute partie agissant en notre nom, les membres de notre joint-venture, nos sous-traitants, nos actionnaires directs ou indirects, et nos filiales, autorisons l'AFD à mener des enquêtes et, en particulier, à inspecter les documents et pièces comptables relatifs à la passation et à l'exécution du Contrat, y compris, mais sans s'y limiter, à nos processus et règles internes relatifs au respect des sanctions internationales prononcées par les Nations Unies, l'Union européenne et/ou la France, et à les faire vérifier par des auditeurs nommés par l'AFD.

Nous déclarons que nous avons payé, ou que nous paierons, les commissions, avantages, honoraires, gratifications ou frais liés à la procédure de passation ou à l'exécution du contrat au(x) tiers suivant(s) (par exemple, un intermédiaire/agent) (*) :

Nom du bénéficiaire	Coordonnées de la personne à contacter	Objectif/objet	Montant (indiquer la devise)

(*) : Si aucun montant n'a été payé ou n'est à payer, indiquer « Aucun ».

Nous reconnaissons que la participation de l'AFD au financement du Contrat est soumise à la Politique de prévention et de lutte contre les Pratiques Prohibées du Groupe AFD.

[1] Disponible sur https://www.afd.fr/en

Nous reconnaissons que l'AFD ne sera pas en mesure de participer au financement du Contrat si nous, y compris toute partie agissant en notre nom[2], tout membre de notre joint-venture, tout fournisseur, contractant, sous-traitant, consultant ou sous-consultant, tout actionnaire direct ou indirect, ou toute filiale agissant :

- sont directement ou indirectement soumis, contrôlés par une personne ou une entité soumise ou agissant au nom ou pour le compte d'une personne ou d'une entité soumise à des sanctions financières adoptées par les Nations Unies, l'Union européenne et/ou la France[3].
- sont directement ou indirectement soumis, contrôlés par une personne ou une entité soumise, ou agissant au nom ou pour le compte d'une personne ou d'une entité soumise à des sanctions sectorielles adoptées par les Nations Unies, l'Union européenne[4] et/ou la France.
- Dans le cadre de l'exécution du Contrat, acquérir ou fournir des biens faisant l'objet d'un embargo adopté par les Nations Unies, l'Union européenne et/ou la France[5].

Nous nous engageons à informer sans délai l'Administration contractante, qui informera l'AFD, de tout changement de circonstances concernant les sections ci-dessus après la signature de la présente Convention.

Nom: _____ En qualité de : _____

Dûment habilité à signer au nom et pour le compte de[6]:_____

Signature_____ Date: _____

---

[2] Les dirigeants (y compris toute personne membre de l'organe d'administration, de direction ou de surveillance, ou ayant un pouvoir de représentation, de décision ou de contrôle), les employés ou les agents (qu'ils soient déclarés ou non).

[3] Les références ou adresses de sites Internet suivantes sont fournies à titre d'information uniquement :
Pour la liste tenue par les Nations unies, l'Union européenne et la France, le site Internet suivant peut être consulté : https://gels-avoirs.dgtresor.gouv.fr/List

[4] Pour information uniquement, les sanctions sectorielles de l'UE sont disponibles à l'adresse suivante : https://www.sanctionsmap.eu/#/main

[5] Pour information uniquement, les sanctions sectorielles de l'UE sont disponibles à l'adresse suivante : https://www.sanctionsmap.eu/#/main

[6] En cas de joint-venture, le nom de la joint-venture doit être inséré ici et la personne dûment autorisée à signer la demande, l'offre ou la proposition au nom du demandeur, du soumissionnaire, de l'offrant ou du consultant doit signer la convention.

Termes De Références

Étude de faisabilité : Développement d'une feuille de route pour la mise en œuvre de la signature électronique en RDC.

ZR-CI-492434-CS-CQS

Octobre 2025

Table des matières

I. INTRODUCTION 3
II. CONTEXTE ET JUSTIFICATION DE LA MISSION 4
III. OBJECTIFS DE L'ETUDE 7
IV. ACTIVITES A REALISER 8
V. CALENDRIER ET LIVRABLES DE LA MISSION 17
VI. SUIVI ET ÉVALUATION 18
VII. INTRANTS FOURNIS PAR LE BENEFICIAIRE 18
VIII. RÉSULTATS ATTENDUS 18
IX. LIEU ET DURÉE DE LA MISSION. 19
X. PROFIL DU CABINET ET DES EXPERTS CLES 19

I. INTRODUCTION

Le Gouvernement de la République Démocratique du Congo (RDC) a reçu un appui de l'Association Internationale pour le Développement (IDA) du Groupe de Banque Mondiale et Agence Française de Développement (AFD) pour réaliser le *Projet de Transformation Numérique (PTN) de la RDC* (« le Project »), qui sera mis en œuvre entre 2025 et 2029.

L'objectif de développement du Projet est d'accroître l'accès et l'utilisation de l'internet et renforcer les bases des services numériques en RDC. Pour ce faire, le Projet investira dans (i) l'infrastructure de connectivité numérique fondamentale nécessaire pour soutenir le mouvement vers l'accès numérique universel ; (ii) l'infrastructure publique numérique (DPI) requise pour permettre aux secteurs publics et privés de développer des services numériques intégrés, ouverts et sécurisés au niveau sectoriel ; (iii) le renforcement de la base de compétences numériques avancée et l'écosystème d'innovation numérique de la RDC pour garantir l'utilisation productive de la technologie, favorisant la création d'emplois et soutenant le développement de nouveaux services numériques, et (iv) le renforcement de la capacité institutionnelle et la gouvernance nécessaires pour mener ces initiatives de manière concertée et intégrée.

Le Projet est constitué de composantes réparties de la manière suivante :

- Composante 1 - Élargir l'accès et l'inclusion numériques : Cette composante soutiendra le développement de cadres favorables et fournira un financement pour compléter et catalyser les investissements du secteur privé dans le déploiement d'infrastructures de réseaux à large bande, en vue d'accélérer les progrès de la RDC vers l'accès universel au haut débit et une inclusion numérique plus large, à travers l'extension du backbone fibre optique nationale et la connectivité rurale.

- Composante 2 - Introduction de bases numériques pour la prestation de services : Cette composante soutiendra les investissements dans les infrastructures et plateformes numériques partagées nécessaires pour étendre la fourniture de services numériques à travers la RDC, tout en soutenant leur intégration dans les secteurs clés pour améliorer l'accès aux services. Elle se concentrera sur les éléments fondamentaux de l'infrastructure DPI qui permettraient au gouvernement de favoriser l'innovation et d'étendre son utilisation des outils numériques.

- Composante 3 - Développer une main-d'œuvre compétente et stimuler l'innovation dans les services numériques : Cette composante visera à mettre en œuvre des programmes de formation pour renforcer les capacités des fonctionnaires, des étudiants et des entrepreneurs engagés dans des programmes dans le domaine de la technologie, en stimulant les liens entre le secteur de l'enseignement supérieur et le secteur technologique, et en alimentant le développement de solutions numériques locales pour une utilisation productive de la technologie numérique.

- Composante 4 - Coordination institutionnelle et gestion du projet : Cette composante financerait la gestion et la coordination du projet du bénéficiaire en matière de

capacités, y compris la passation des marchés, la gestion financière, le suivi et l'évaluation, ainsi que la gestion des aspects environnementaux et sociaux (E&S).

La mise en œuvre est dirigée par le ministère des Postes et Télécommunications (MPT), où une Unité de Gestion du Projet a été créée, en collaboration avec d'autres parties prenantes, telles que l'Autorité de Régulation des Postes, des Télécommunications et des Technologies de l'Information et de la Communication (ARPTIC), le Fonds de développement des services universels (FDSU), le ministère de l'Économie Numérique, ministère de l'Intérieur, ministère de l'Enseignement supérieur et universitaire, ministère de l'Industrie et des PME, etc.

Pour plus de détails sur le Projet, veuillez consulter le document du projet : https://documents1.worldbank.org/curated/en/099061024103010133/pdf/BOSIB130fc11f60601aa191c219a13fc1e5.pdf - veuillez-vous référer à l'annexe 3 pour une description du projet en RDC.

Dans le cadre de la Composante 2 du Projet, un appui est prévu pour l'élaboration et la mise en œuvre d'une feuille de route pour l'adoption des signatures électroniques dans les secteurs public et privé, y compris des processus de certification pour les signatures électroniques qualifiées, sur la base de transactions de cas d'utilisation classés par ordre de priorité.

II. CONTEXTE ET JUSTIFICATION DE LA MISSION

Clarification conceptuelle

Il est essentiel de distinguer dès le départ deux notions souvent confondues :

- **La signature électronique** : terme générique qui désigne tout procédé électronique permettant de manifester le consentement d'une partie à un acte ou à un document. Selon le niveau de sécurité, elle peut être simple, avancée ou qualifiée. Elle constitue une catégorie large, qui regroupe divers mécanismes permettant d'authentifier des transactions ou documents numériques.
- **La signature numérique** : sous-catégorie spécifique de la signature électronique, reposant sur la cryptographie asymétrique et l'utilisation de certificats délivrés par une infrastructure à clés publiques (PKI). Elle assure un haut niveau de sécurité, d'authenticité et d'intégrité, et correspond généralement aux signatures électroniques qualifiées prévues par le Code du Numérique en RDC.

Importance de la e-signature

Alors que le monde devient de plus en plus numérique, le besoin de méthodes sûres, efficaces, utilisables et légalement reconnues devient de plus en plus important. Les signatures électroniques sont un élément clé des transactions numériques, car elles permettent aux parties d'interagir en ligne tout en ayant la certitude d'être protégées contre les différents types de fraude qui peuvent affecter les interactions numériques. De ce fait, elles forment une infrastructure sous-jacente fondamentale pour assurer la confiance dans les transactions en ligne et l'utilisation des services numériques.

Dans le fonctionnement au quotidien de l'administration publique autant que dans le secteur privé, de nombreuses interactions font l'objet de signatures, numérisées ou non (correspondance administrative, procès-verbal, convention/contrat, consentement,

authentification, etc.). Les signatures électroniques peuvent garantir l'identité des parties à une transaction et protéger l'intégrité d'une transaction en empêchant la modification a posteriori de détails importants, tels que les termes du contrat ou les montants de la transaction.

Parallèlement à d'autres techniques d'authentification des transactions électroniques, les signatures électroniques sont un élément essentiel de l'évolution vers des environnements sans papier, car elles permettent de réduire les coûts et de rationaliser les processus dans les secteurs privé et public. Les signatures électroniques sont un des éléments fondamentaux au sein d'une infrastructure DPI, et forment une des bases nécessaires pour le développement de plateformes de partage de données, de portefeuilles numériques ou d'autres systèmes d'identification décentralisés. Elles jouent un rôle clé pour améliorer l'expérience des utilisateurs de services dans des domaines comme la santé, l'éducation, le commerce électronique, et aident à faciliter l'expansion de l'économie numérique de manière générale.

Les signatures électroniques pour des transactions à risque faible ou moyen sont souvent conçues autour de la composante d'identité plutôt que d'une infrastructure à clé publique (« PKI »). Par ailleurs, le terme « signature numérique » fait généralement référence exclusivement aux signatures basées sur des certificats numériques délivrés et gérés par une PKI. Les technologies cryptographiques telles que le PKI sont normalement réservées aux cas d'utilisation à haut risque, lorsqu'il est nécessaire de pouvoir vérifier l'intégrité du texte précis de l'ordre de virement, ou son horodatage précis, afin d'assurer la sécurité de la transaction.

Situation actuelle en RDC

En RDC, l'utilisation de la signature électronique (et signature numérique) reste limitée, ce qui freine la mise en œuvre du programme d'e-Gouvernement congolais, et le développement de services numériques dans le secteur privé, qui pourraient améliorer la participation à l'économie numérique, renforcer la transparence et lutter contre la fraude. Les signatures électroniques pourraient par exemple favoriser l'inclusion financière à travers le développement de la banque numérique et du commerce électronique. De même, dans le secteur public et dans le cadre du programme d'e-Gouvernement congolais, les signatures électroniques fiables sont nécessaires pour la mise en œuvre des projets de guichet unique, d'état civil numérique, de passation des marchés publics, de systèmes fiscaux. Elles pourraient ainsi rendre ces services plus accessibles et plus efficaces en réduisant les obstacles bureaucratiques et en améliorant la transparence. Cependant, la mise en œuvre des signatures électroniques en RDC s'accompagne également de défis uniques, tels que la faible capacité institutionnelle au sein d'un écosystème de gouvernance en phase de transition, les nombreux obstacles à l'adoption de solutions numériques avancées, comme la connectivité, les compétences numériques, et la culture numérique des utilisateurs.

En 2023, le gouvernement a adopté un nouveau Code du Numérique pour favoriser la confiance des citoyens et des entreprises dans les échanges numériques, qui comprend des dispositions pour les signatures électroniques, ainsi que l'établissement d'une autorité de certification (*Ordonnance-loi n°23-010 du 13 mars 2023*).

Sous le Code du Numérique de la RDC, deux niveaux de signatures électroniques (simples et qualifiées) sont introduits, garantissant l'intégrité des documents électroniques et l'identité des signataires (Article 104 à 117). Les signatures qualifiées, soutenues par des certificats délivrés

par des prestataires de confiance accrédités, offrent la même valeur probante que les signatures manuscrites (Articles 108 et 115) et sont essentielles pour les transactions à haut risque. Actuellement, aucune réglementation, procédure ou infrastructure technologique n'a été mise en place pour mettre en œuvre les dispositions de la loi et favoriser l'utilisation plus large des signatures électroniques, y compris l'infrastructure cryptographique nécessaire pour la signature électronique qualifiée.

Plus spécifiquement, le Code du Numérique (Article 9 et 10) prévoit la création d'une Autorité Nationale de Certification Électronique (ANCE) chargée de fixer les caractéristiques du dispositif de création et de vérification de la signature électronique, de gérer l'infrastructure à clés publiques nationale, et de délivrer les certificats électroniques. Cependant, l'absence de réglementation et d'opérationnalisation de l'ANCE limite la mise en œuvre pratique des dispositions légales et entrave l'établissement de cet écosystème essentiel pour l'adoption des signatures électroniques, soulignant l'urgence d'établir un cadre réglementaire, institutionnel pour garantir leur fiabilité et leur sécurité. Ce cadre de gouvernance est indispensable pour instaurer la confiance dans l'usage des signatures électroniques, particulièrement des signatures numériques, qui nécessitent souvent la coordination entre multiples acteurs.

La mise en œuvre de ce cadre de gouvernance doit inclure :

1. L'élaboration et la promulgation des textes réglementaires spécifiques nécessaires pour opérationnaliser les dispositions du Code du Numérique, conformément aux Articles 9, 10, 14 et 176.
2. La mise en place des structures institutionnelles, notamment l'ANCE et l'Agence Nationale de Cybersécurité, conformément aux prévisions des Articles 9, 10 et 274.
3. Le développement des capacités techniques et institutionnelles, incluant la formation et la sensibilisation des utilisateurs, pour promouvoir l'adoption des signatures électroniques et garantir leur utilisation sécurisée, conformément aux objectifs définis dans l'Article 193 du Code.

L'absence d'un cadre de gouvernance comprenant les textes réglementaires visant l'application du Code du Numérique ainsi que l'écosystème institutionnel adéquat pour instaurer la confiance dans l'usage des signature électroniques limite la capacité des acteurs économiques, dont notamment les investisseurs et les PME congolaises, à mener des transactions sécurisées en RDC afin de mieux participer aux chaines d'approvisionnement régionales et mondiales. Ce vide freine également l'adoption des autres éléments fondamentaux de l'infrastructure DPI, tels que l'identification numérique, le partage des données, l'interopérabilité des systèmes et les systèmes de paiement instantanés et sécurisés qui pourraient transformer les secteurs public et privé.

Néanmoins, afin de préparer la mise en œuvre opérationnelle du système de certification électronique, le gouvernement a autorisé, par un arrêté ministériel du MPTN pris en 2024, l'ARPTIC à procéder à la préparation de la mise en place de certaines de ces dispositions à titre provisoire en matière de certification électronique.

III. OBJECTIFS DE L'ETUDE

L'objectif global de l'étude de faisabilité est de permettre la mise en place d'un cadre robuste pour la gouvernance et l'opérationnalisation des signatures électroniques, sur la base d'une feuille de route détaillée, budgétisée et séquencée, permettant à la RDC de déployer d'ici 2030 une infrastructure nationale de signature électronique fiable, interopérable et économiquement soutenable, en pleine conformité avec le Code du Numérique, les normes internationales.

Les objectifs spécifiques sont les suivants :

1. Évaluer le cadre légal, réglementaire et institutionnel existant (Code du Numérique, textes OHADA, régulations sectorielles), les infrastructures et systèmes existants, ainsi que l'utilisation projetée des signatures électroniques et services de confiance dans les secteurs public et privé.
2. Mobiliser et consulter les parties prenantes en impliquant les acteurs publics et privés afin de créer un écosystème favorable au développement des services de confiance, et clarifier leurs rôles, mandats, modèles de fonctionnement et indicateurs de performance (KPI).
3. Déterminer les préconditions nécessaires et identifier et formaliser les conditions juridiques, institutionnelles, techniques et organisationnelles requises pour établir et reconnaître les signatures électroniques simples et qualifiées.
4. Proposer un cadre juridique optimal avec des recommandations pour compléter, harmoniser et opérationnaliser le cadre légal et réglementaire existant, y compris la rédaction ou la mise à jour des textes secondaires nécessaires (décrets, arrêtés, directives techniques), et garantir la conformité aux normes internationales pertinentes, notamment pour faciliter l'interopérabilité transfrontalière des services de confiance.
5. Concevoir le modèle organisationnel et opérationnel, y compris la gouvernance, les processus de supervision et d'audit, ainsi que les mécanismes de redevance pour l'Autorité Nationale de Certification Électronique (ANCE) et les fournisseurs de services de confiance (FSC). (à réaliser en collaboration ou dans la continuité, selon le cas, de ce que les institutions gouvernementales ont déjà entrepris)
6. Définir l'architecture technique cible, en élaborant les scénarios et spécifications techniques de l'infrastructure nécessaire à la mise en œuvre et à l'interopérabilité des signatures électroniques qualifiées, incluant les exigences de cybersécurité, d'intégration avec l'identité numérique et d'interopérabilité avec les systèmes d'information publics et privés.
7. Analyser la viabilité économique et financière du projet en estimant les coûts d'investissement et d'exploitation (CAPEX/OPEX), et proposant un plan de financement durable (« business model ») combinant ressources publiques, partenariats techniques et modèles "pay-as-you-grow".
8. Identifier les cas d'usage prioritaires à forte valeur ajoutée pour un déploiement rapide dans le secteur public (ex. e-procurement, état civil numérique, fiscalité) et privé, et définir les actions techniques, réglementaires et opérationnelles nécessaires à leur mise en œuvre.

9. Renforcer les capacités et sensibiliser les parties prenantes en concevant et mettant en œuvre un plan de formation et de communication ciblant régulateurs, administrations, prestataires et usagers afin de favoriser l'adoption et la confiance dans le système.
10. Élaborer la feuille de route nationale 2026-2030 avec un plan opérationnel séquencé, assorti de jalons, livrables, indicateurs de performance, priorités à court terme ("quick wins") et mécanismes de suivi-évaluation pour le déploiement national des signatures électroniques, y compris des plans sur la manière de soutenir l'introduction d'une autorité de certification et d'une infrastructure PKI pour les transactions à haut risque.
11. Préparer les cahiers des charges, spécifications techniques et autres documents nécessaires aux procédures de passation de marchés pour l'acquisition, l'intégration et l'exploitation des composantes techniques de l'infrastructure de confiance.

La mission est proposée en trois volets : A) État des lieux et diagnostic de l'existant, B) Conception du cadre de gouvernance et de l'architecture cible, et C) Préparation opérationnelle et feuille de route.

N.B.
Le consultant devra également collaborer pour s'aligner avec d'autres cabinets menant des études et des projets similaires ou connexes en RDC et financés par le projet sur l'administration en ligne, l'assistance juridique, et la gouvernance des données.

IV. ACTIVITES A REALISER

La mission débutera par une courte phase de démarrage visant à clarifier la méthodologie à utiliser, le calendrier de travail et le plan de mobilisation des parties prenantes (gouvernement, régulateur, secteurs régulés, entreprises du secteur privé, société civile). Elle débouchera sur un rapport de démarrage définissant le périmètre, la méthode, le planning et les principaux risques de la mission.

Livrable 0 : Rapport de démarrage

A) ETAT DES LIEUX ET DIAGNOSTIC DE L'EXISTANT

Activité 1 : Analyse du cadre institutionnel, juridique et réglementaire

Analyser les lois, règlements et politiques qui traitent spécifiquement de la validité, de la reconnaissance et de l'utilisation des signatures électroniques ou qui ont un impact sur celles-ci, et identifier les lacunes susceptibles d'entraver l'utilisation et la reconnaissance effectives des signatures électroniques :

- Analyser le cadre juridique et institutionnel existant (Code du numérique, textes OHADA, régulations sectorielles) en ce qui concerne les signatures électroniques. *
- Identifier les lacunes à combler pour soutenir la mise en œuvre et s'aligner sur les cadres de bonnes pratiques comme UNCITRAL (modèles de lois sur signature électronique) et Règlement (UE) eIDAS.
- Évaluer les options d'harmonisation du cadre juridique avec d'autres pays africains et entités internationales en matière d'interopérabilité transfrontalière des services numériques.

- Formuler des recommandations sur les modifications à apporter au cadre juridique et institutionnel pour poser les bases d'une approche fondée sur les risques et permettre une adoption plus large des signatures numériques tout en garantissant un niveau de sécurité adapté pour chaque type de transaction.

Livrable 1 : Rapport de diagnostic juridique et institutionnel

**NB : Une analyse préliminaire pourrait être disponible dans le cadre d'une mission parallèle visant à aider le gouvernement à harmoniser la loi de 2020 sur les télécommunications et le code numérique de 2023, et à élaborer une législation secondaire pour soutenir la mise en œuvre de ces lois.*

Activité 2 : Analyser la capacité actuelle et future en fonction des besoins projetés

Faire l'inventaire des infrastructures et système techniques existants pertinents (PKI, gestion d'identité, systèmes publics et privés) et évaluer leur adoption actuelle et la demande future d'e-signature par les entités privées et publique pour les transactions, y compris pour les transactions transfrontalières :

- Cartographier les principales parties prenantes impliquées dans la gouvernance, la mise en œuvre et l'utilisation des signatures électroniques, telles que les autorités de réglementation gouvernementale, les fournisseurs de services de confiance (FSC), les entreprises du secteur privé et les utilisateurs finaux.
- Recueillir les attentes et besoins des parties prenantes, y compris les institutions publiques, les entreprises et les citoyens, à travers des ateliers, entretiens ou consultations, garantissant que les points de vue de toutes les parties concernées soient pris en compte.
- Évaluer et cartographier les infrastructures et systèmes techniques (data centers, plateformes d'identité, réseaux GovNet, projet e-Gouvernement) ayant trait à l'adoption de la signature électronique, ainsi que la capacité institutionnelle pour les mettre en œuvre, particulièrement en termes de sécurité et d'interopérabilité. **
- Analyser la base d'utilisateurs et les solutions techniques existantes ou envisagées, afin d'évaluer les besoins spécifiques et les barrières potentielles à l'adoption.
- Identifier et classer de façon exhaustive les principaux cas d'utilisation en fonction des risques pouvant faire l'objet de signature électronique simple, et ceux pouvant faire l'objet d'une certification.
- Identifier les points d'entrée et des recommandations sur la manière d'inciter les secteurs public et privé à utiliser pour les cas d'utilisation identifiés en matière de signature électronique et de certification.
- Prendre en compte les exigences d'utilisabilité, notamment pour garantir que les solutions proposées soient accessibles et adaptées à divers profils d'utilisateurs.
- Établir des cas d'utilisation prioritaires pour les signatures électroniques, en identifiant ceux ayant un impact élevé et une utilisation potentielle significative dans les secteurs publics et privés.

***NB : Une autre entreprise cartographiera en détail tous les systèmes et infrastructures gouvernementaux, en vue d'élaborer une feuille de route intégrée pour l'administration électronique, y compris une architecture d'entreprise gouvernementale globale, tandis que d'autres entreprises seront engagées pour évaluer et concevoir les dispositifs d'hébergement des données du gouvernement et pour*

concevoir un système d'identification de base. Cette mission devrait simplement consister à dresser un inventaire de haut niveau afin d'identifier comment la signature électronique dépendra de ces éléments et interagira avec eux, lors de la conception d'un plan de mise en œuvre par étapes.

Livrable 2 : Rapport de cartographie de l'écosystème

B) CONCEPTION DU CADRE DE GOUVERNANCE ET ARCHITECTURE CIBLE

Activité 3 : Scénarios d'architecture et analyse multicritère

Réaliser une analyse comparative et un examen des options pour l'architecture cible déterminant le choix des spécifications techniques pour intégrer la signature électronique simple et qualifiée dans la prestation de services numériques, et recommander une option optimale en fonction de critères techniques, opérationnels, juridiques, économiques et sécuritaires.

- Faire un benchmark des modèles adoptés par différents pays (par exemple Estonie et le Brésil, etc.) et comparer les cadres envisagés avec les meilleures pratiques et normes internationales, en s'appuyant notamment sur des instruments de référence tels que la Loi type de la CNUDCI sur l'utilisation et la reconnaissance internationale de la gestion de l'identité et des services de confiance, ainsi que sur les cadres régionaux pertinents (par ex. Union africaine, CEDEAO, SADC). L'analyse pourra également inclure, à titre comparatif, des expériences internationales reconnues (par ex. règlement eIDAS de l'Union européenne), en veillant à évaluer leur pertinence et adaptabilité au contexte africain et congolais.
- Adopter une approche fondée sur les risques, équilibrée par des considérations d'utilisabilité, pour garantir que les solutions proposées s'adaptent aux niveaux de sensibilité et de sécurité requis tout en restant accessibles et pratiques pour les utilisateurs.
- Établir des synergies entre signature électronique et systèmes d'identité numérique, dans le but d'appuyer une gouvernance robuste, des mécanismes d'interopérabilité et des modes d'accès aux services (portails citoyens, etc.) pouvant soutenir directement l'adoption intégrée des signatures électroniques dans une approche DPI.
- Identifier et analyser les options disponibles en fonction de leur viabilité économique et d'autres facteurs tels que la capacité institutionnelle, les compétences numériques, la disponibilité de personnel qualifié, l'offre du marché, l'infrastructure (telles que la connectivité et l'hébergement de données, réseaux d'enregistrement), ainsi que l'accès aux équipements nécessaires (ordinateurs, smartphones, tablettes, etc.) pour garantir une adoption large et inclusive des signatures électroniques.
- Pour la signature électronique qualifiée, explorer les différentes architectures et modèles d'approvisionnement disponibles pour le déploiement du PKI tout en tenant compte de facteurs tels que la capacité de mise à l'échelle.
    - Modèles d'architecture PKI : simple ; deux niveaux ; trois niveaux ;
    - Modèles de déploiement : sur site, cloud, hybride.
- Analyser les possibilités d'émergence d'écosystèmes de FSC qualifiés dans le secteur privé.Réaliser une analyse multicritère (technique, opérationnelle, juridique, économique et sécuritaire) pour comparer et recommander l'option optimale entre les

recommandations faites. Les investissements proposés doivent être basés sur la demande prévue, et permettre une mise à l'échelle et une adaptation progressive.

- Organiser un atelier pour discuter des principaux résultats analytiques et présenter les options.
- Définir les spécifications techniques cibles pour l'option recommandée.
- Définir les besoins techniques et les exigences de sécurité pour les technologies de signature électronique, y compris des mécanismes d'authentification, des normes d'interopérabilité, des techniques de cryptage, l'émission, la gestion et l'utilisation des certificats numériques. Celles-ci devront prendre en compte les exigences en matière de cybersécurité, d'intégration avec le cadre de l'infrastructure DPI, de l'identité numérique, et de l'interopérabilité avec les secteurs publics et privés.

Livrable 3.a : Note comparative de scénarios
Livrable 3.b : Atelier de validation des options
Livrable 3.c : Spécifications techniques pour l'option recommandée

Activité 4 : Proposer un cadre juridique optimal

Sur la base de l'option optimale validée, proposer un cadre juridique optimal en lien avec le Code du Numérique et les bonnes pratiques et normes internationales pour assurer l'interopérabilité transfrontalière sur le continent africain et au niveau global.

- Effectuer des recommandations de textes législatifs et réglementaires secondaires à introduire (décrets, arrêtés, directives et règlements techniques). Si certains textes existent déjà, le consultant peut également donner son avis sur ceux-ci en vue de leur finalisation. Toutefois, l'élaboration d'autres textes manquants nécessaires au bon fonctionnement pourrait s'avérer nécessaire***.
- Élaborer des projets d'amendements juridiques et des projets de réglementation prêts à consultation avec les parties prenantes, en s'appuyant aussi sur les résultats de l'analyse juridique et harmonisation des textes.

****NB : Comme indiqué ci-dessus, certains textes juridiques peuvent déjà être disponibles sur la base d'une mission juridique parallèle.*

Livrable 4 : Paquet juridique de notes réglementaires et projets de textes secondaires.

Activité 5 : Proposer un cadre de gouvernance avec un modèle organisationnel économiquement soutenable

Établir un « blueprint » de l'écosystème des services de confiance en RDC en formalisant les mandats et modèles d'organisation des principaux acteurs, notamment concernant les missions, processus, staffing et formation de l'ANCE, ainsi que les modèles économiques et financiers sous-jacents.

- Détailler les cadres institutionnels et administratifs à mettre en place pour la gestion pérenne, en examinant les personnes et les processus, en proposant la création ou la désignation d'organismes nationaux chargés de superviser le cadre de la signature électronique (pour la décision finale du gouvernement), y compris en appuyant des

autorités réglementaires, de certification et d'enregistrement, ou service de vérification d'identité, dont notamment :

- L'Autorité Nationale de Certification Électronique (ANCE) pour superviser et délivrer les certificats électroniques, fournir des orientations sur l'utilisation de la signature électroniques,

- Définir les rôles, les responsabilités et les relations entre les principales institutions et parties prenantes.
- Définir les profils types de cadres à travailler dans cette institution, y compris les responsabilités.
- Identifier et structurer les mandats et protocoles des acteurs institutionnels liés à la supervision et à l'audit des parties prenantes pour garantir la conformité aux réglementations et à l'engagement des parties prenantes, y compris les entreprises privées, les PME, les autorités publiques et les utilisateurs finaux.
- Fournir des lignes directrices pour le règlement des litiges et les mécanismes de recours liés aux transactions de signature électronique, en veillant à ce que le cadre et les lignes directrices s'adressent à la fois aux grandes entreprises et aux PME des différents secteurs.
- Proposer des mécanismes de mise à jour et de révision réguliers des lignes directrices afin de s'adapter aux progrès technologiques et aux nouveaux défis.
- Sur le plan organisationnel, analyser les coûts d'investissement et d'exploitation (CAPEX/OPEX) des acteurs du secteur basé sur la demande, et définir un plan de financement durable pour l'ANCE combinant la mobilisation des ressources domestiques et la participation du secteur privé et des partenaires techniques.

Livrable 5.a : Rapport de modèle organisationnel et économique
Livrable 5.b : Lignes directrices et protocoles pour l'audit des acteurs et le règlement des litiges
Livrable 5.c : Plan de financement et budget consolidé de l'ANCE

Activité 6 : Cadre de gestion du risque et conformité

En fonction des modèles techniques choisis et des cas d'utilisation prioritaires, présenter les options pour différents niveaux de risque ainsi qu'un plan de mitigation.

- Dresser une cartographie des menaces (NIST Cyber Security Framework) et des vecteurs de fraude. Lister les conditions préalables, des opportunités, des défis et des risques liés à chaque élément du système considéré.
- Intégrer des mesures visant à protéger les droits et la vie privée des utilisateurs, y compris des mécanismes de consentement, des exigences de transparence et des normes de protection des données, et atténuer les risques potentiels associés à la mise en œuvre, tels que les cyberattaques.
- Pour les cas d'utilisation à haut risque, présenter au moins trois (03) solutions de certification ayant fait leur preuve et la solution la mieux adaptée au contexte congolais est réalisée. Les solutions proposées doivent (i) être adaptées à un contexte de développement caractérisé par des contraintes en matière d'infrastructures et de capacités, (ii) mettre en balance la facilité d'utilisation et les considérations de sécurité ; (iii) être centrées sur l'utilisateur et basées sur les points de contact existants avec les citoyens et les clients.

Livrable 6 : Cadre de gestion des risques et conformité

C) FEUILLE DE ROUTE ET PREPARATION OPERATIONNELLE

Activité 7 : Élaboration de la feuille de route

La feuille de route de mise en œuvre de la signature électronique sur la base des éléments techniques et analytiques ci-dessus, autour desquels elle offrira des recommandations claires sur les étapes à suivre, les principaux jalons et les investissements nécessaires pour parvenir à l'opérationnalisation et à l'adoption d'un cadre de confiance autour des signatures numériques en RDC. Elle identifiera les mesures nécessaires pour garantir que les signatures numériques congolaises suivent les pratiques internationalement reconnues tout en s'adaptant au contexte local, en commençant par les secteurs tirés par une forte demande, où l'usage et l'impact seraient les plus importants et permettent par la suite de mettre à l'échelle le système sur la base des enseignements tirés.

- Rédiger la feuille de route nationale à horizon 2030 avec jalons, livrables, priorités à court terme, budgets, indicateurs de performance et mécanismes de suivi-évaluation
- Identifier le rôle et la responsabilité pour les actions clés nécessaires à la mise en œuvre de la feuille de route.
- Identifier et formaliser les cas d'usage prioritaires (e-procurement, état civil numérique, fiscalité) avec des ébauches de plans d'implémentation sectoriels.
- Identifier les ressources nécessaires - humaines et financières.
- Établir des indicateurs clairs pour suivre les progrès de la mise en œuvre et évaluer l'impact du cadre de la signature électronique sur les transactions numériques et les activités économiques.
- Identifier les principaux risques associés à la mise en œuvre, ainsi que des stratégies proposées pour les atténuer.
- Analyser les opportunités d'appui par le PTN, en fonction du budget disponible et du calendrier de mise en œuvre du Projet.
- Etablir un plan séquencé comprenant des activités clairement identifiées par « package » qui puisse faire l'objet d'une passation de marché appuyée par le PTN.

Livrable 7 : Feuille de route pour la mise en œuvre de la signature électronique en RDC (livrable principal)

Activité 8 : Plans et documents de passation de marchés

Pour mettre en œuvre la feuille de route, aider le gouvernement à identifier les activités prioritaires que le Projet devrait financer. Cette priorisation devrait prendre en compte les éventuels gains d'efficacité et les synergies avec d'autres activités susceptibles d'être financées (par exemple, entre l'enregistrement de l'ID et du PKI[1]).

- Dresser un plan de passation de marché (phasé) avec la liste et le type d'achats qui seront nécessaires pour appuyer la mise en œuvre (services de conseil, biens,

[1] La coordination de la délivrance des certificats avec l'écosystème national d'identification peut permettre de délivrer des certificats numériques sur la base du même processus de vérification de l'identité que les pièces d'identité ou de tirer parti d'une authentification forte de l'identité numérique pour permettre l'enregistrement en ligne de l'ICP et la distribution des clés sans compromettre la confiance.

formation, etc.). Ce plan devrait être optimisé afin de réduire au minimum le nombre de lots proposés.

- Rédiger les termes de référence, cahiers des charges et spécifications techniques pour les services de conseil, matériels, systèmes et logiciels requis afin de permettre la passation de marchés ultérieurs.
- Le plan de passation de marché devra inclure toute activité liée à l'opérationnalisation de l'ANCE pour mener à bien ses missions établies par la feuille de route.

Livrable 8.a : Plan de passation de marché
Livrable 8.b : Dossiers de documents d'appel d'offres

Activité 9 : Renforcement des capacités, sensibilisation et validation

- Conception d'un programme de formation pour les cadres de l'agence qui seront recrutés.
- Conception d'un programme de renforcement des capacités basiques pour les institutions publiques, les régulateurs, administrations, FSC, et autres parties prenantes clés afin de les accompagner tout au long de l'activité, pour mieux les préparer à mettre en œuvre la feuille de route et opérationnaliser les recommandations autour de l'ANCE et de l'écosystème des services de confiance.
- Identifier les principales parties prenantes nationales devant être informées sur les signatures électroniques et proposer des actions de sensibilisation visant à promouvoir les avantages des signatures électroniques et à encourager leur adoption par les entreprises et le grand public.
- Participer à un atelier de validation et à cinq présentations virtuelles avec les parties prenantes régionales et nationales concernées afin de partager et d'obtenir des commentaires sur les rapports.
- Rédiger un document de synthèse type « policy brief » communiquant les résultats de haut niveau et les messages clés, ainsi que les prochaines étapes/actions adaptées aux différents publics.

Livrable 9.a : Plan de formation
Livrable 9.b : Formation initiale des acteurs clés
Livrable 9.c : Dossier de sensibilisation
Livrable 9.d : Atelier de validation national
Livrable 9.e : Rapport de validation finale et document de synthèse à haut niveau

Tableau 1 : Résumé de la logique d'intervention de la mission

Phase	Activité / Sous-activités	Jalon de validation	Livrables
Phase 0 – Lancement & cadrage	- Réunion de démarrage et clarification de la méthodologie, calendrier et plan de mobilisation des parties prenantes. - Validation du périmètre, de la méthode, du planning et de l'analyse préliminaire des risques.	Validation du rapport de démarrage.	**L0** – Rapport de démarrage (10–15 p.)
Phase A – État des lieux & diagnostic de l'existant	**1. Analyse du cadre institutionnel, juridique et réglementaire** : revue du Code du Numérique, OHADA, régulations sectorielles, identification des lacunes, options d'harmonisation et recommandations. **2. Analyse de la capacité actuelle et future** : cartographie des parties prenantes, besoins et attentes, inventaire PKI et systèmes liés, analyse des solutions existantes, identification préliminaire des cas d'usage prioritaires.	Validation du diagnostic complet avant lancement des scénarios techniques.	**L1** – Rapport de diagnostic juridique et institutionnel (~30 p.) **L2** – Rapport de cartographie d'écosystème (~30 p.)
Phase B – Conception du cadre cible	**3. Scénarios d'architecture et analyse multicritère** : benchmark international, analyse des options PKI, spécifications techniques, exigences de sécurité et d'interopérabilité, analyse multicritère, atelier de validation. **4. Cadre juridique optimal** : recommandations de textes secondaires, projets d'amendements réglementaires prêts à consultation. **5. Cadre de gouvernance et modèle économique** : rôles institutionnels, organisation ANCE/FSC, protocoles d'audit/litiges, modèle financier et plan de financement durable.	Validation du scénario et de l'architecture cible + accord sur le cadre juridique et institutionnel avant élaboration de la feuille de route.	**L3.a** – Note comparative de scénarios (~20 p.) **L3.b** – Atelier de validation des options **L 3.c** : Spécifications techniques pour l'option recommandée **L4** – Paquet juridique et projets de textes secondaires (~40 p.) **L5.a** – Note de modèle organisationnel et économique (~25 p.)

Phase	Activité / Sous-activités	Jalon de validation	Livrables
	6. Cadre de gestion des risques et conformité : cartographie des menaces, solutions pour cas d'usage à haut risque, mesures de protection des données et cybersécurité.		**L5.b** – Lignes directrices et protocoles audit/litiges (~10 p.) **L5.c** – Plan de financement et budget consolidé de l'ANCE (~5 p.) **L6** – Cadre de gestion des risques et conformité (10–15 p.)
Phase C – Feuille de route & préparation opérationnelle	**7. Élaboration de la feuille de route** : plan national 2025–2029 avec jalons, budgets, indicateurs, quick wins, introduction ANCE et PKI pour transactions à haut risque, plans sectoriels par cas d'usage prioritaire. **8. Plans et documents de passation** : plan d'achats, termes de référence, cahiers des charges et spécifications techniques pour mise en œuvre. **9. Renforcement des capacités, sensibilisation et validation** : plan de formation, sessions initiales, dossier de communication, atelier national de validation, policy brief.	Validation finale de la feuille de route et du package opérationnel complet.	**L7** – Feuille de route (~60 p.) **L8.a** – Plan de passation de marché (~3 p.) **L8.b** – Dossiers d'appel d'offres (30–50 p.) **L9.a** – Plan de formation (5–10 p.) **L9.b** – Formation initiale **L9.c** – Dossier de sensibilisation (3–5 p.) **L9.d** – Atelier national de validation **L9.e** – Rapport de validation finale & synthèse (5–10 p.)

V. CALENDRIER ET LIVRABLES DE LA MISSION

La durée totale de la mission est de cent quarante (**140) jours** calendaires à compter de la date d'attribution de la mission.

A) ETAT DES LIEUX ET DIAGNOSTIC DE L'EXISTANT		
L0 : Rapport de démarrage (10-15p)	Semaine 2	10%
L1 : Rapport de diagnostic juridique et institutionnel (~30p)	Semaine 6	20%
L2 : Rapport de cartographie d'écosystème (~30p)	Semaine 8	
B) CONCEPTION DU CADRE DE GOUVERNANCE ET ARCHITECTURE CIBLE		
L3.a : Note comparative de scénarios (~20p)	Semaine 10	25%
L3.b : Atelier de validation des options	Semaine 10	
Livrable 3.c : Spécifications techniques pour l'option recommandée	Semaine 12	
L4 : Paquet juridique de notes réglementaires et projets de textes secondaires (~40p)	Semaine 12	
L5.a : Rapport de modèle organisationnel et économique (~25p)	Semaine 13	15%
L5.b : Lignes directrices et protocoles pour l'audit des acteurs et le règlement des litiges (~10p)	Semaine 13	
L5.c : Plan de financement et budget consolidé de l'ANCE (~5p)	Semaine 13	
L6 : Cadre de gestion des risques et conformité (10-15p)	Semaine 14	
C) FEUILLE DE ROUTE ET PREPARATION OPERATIONNELLE		
L7 : Feuille de route pour la mise en œuvre de la signature électronique en RDC (livrable principal) (~60p)	Semaine 16	30%
L8.a : Plan de passation de marché (~3p)	Semaine 18	
L8.b : Dossiers de documents d'appel d'offres (~30-50p)	Semaine 18	
L9.a : Plan de formation (~5-10p)	Semaine 18	
L9.b : Formation initiale des acteurs clés	Semaine 18	
L9.c : Dossier de sensibilisation (~3-5p)	Semaine 18	
L9.d : Atelier national de validation	Semaine 19	
L9.e : Rapport de validation finale et document de synthèse à haut niveau (~5-10p)	Semaine 20	

Chaque « rapport » sera fourni en français au format WORD et sera accompagné d'un résumé exécutif Powerpoint synthétisant les points essentiels du rapport.

VI. SUIVI ET ÉVALUATION

Le Consultant rendra compte de tous les livrables indiqués ci-dessus au Coordonnateur de l'Unité de Gestion du PTN. Chaque livrable fera l'objet d'une réunion de validation (il sera possible de combiner plusieurs livrables). La validation des livrables sera faite par le comité technique de suivi pour évaluer l'avancement de l'étude et la qualité des résultats obtenus.

VII. INTRANTS FOURNIS PAR LE BENEFICIAIRE

Le maitre d'ouvrage mettra à la disposition du soumissionnaire retenu :

- Toute la documentation jugée utile par le soumissionnaire dont il dispose ;
- Toutes les facilités d'accès aux informations souhaitées ;
- Un point focal pour tout besoin d'information.
- Toute la documentation jugée pertinente pour la réalisation ou l'information de la mission et l'accomplissement des tâches identifiées, dont il dispose. Cela comprend par exemple les documents politiques clés et les textes juridiques.
- L'accès aux principaux responsables des ministères/agences/départements concernés et autres entités officielles pertinentes, le cas échéant.
- Faciliter la coopération avec d'autres organisations, dont les activités et les programmes peuvent être considérés comme pertinents pour la mission. Cela inclut les autres cabinets travaillant sur des missions liées, comme indiqué ci-dessus.
- Les coûts et l'organisation logistique liée à l'organisation des consultations/ateliers et à l'identification des personnes à former, en étroite collaboration avec le consultant.

VIII. RÉSULTATS ATTENDUS

Les résultats attendus au terme de la mission sont les suivants :

1. **Le cadre juridique et réglementaire est renforcé** avec recommandations et projets de textes secondaires alignés sur les normes internationales et facilitant l'interopérabilité transfrontalière.
2. **Un diagnostic complet** du cadre institutionnel, des parties prenantes et des capacités techniques existantes permet de soutenir l'adoption large et inclusive de la signature électronique.
3. **Une architecture technique cible est validée** avec benchmarking, scénarios comparés, spécifications techniques, exigences d'interopérabilité et de cybersécurité.
4. **Un cadre de gouvernance et modèle économique opérationnels sont adoptés, incluant un** plan de financement durable, protocoles d'audit et mécanismes de règlement des litiges.
5. **La feuille de route nationale 2026–2030 est validée** et prête pour mise en œuvre avec un package opérationnel (plan de passation, dossiers d'appel d'offres, plan de formation et sensibilisation), avec une proposition claire des activités réalisables et prioritaires avec le PTN.

IX. LIEU ET DURÉE DE LA MISSION.

La mission se déroulera en République démocratique du Congo, sur une durée de vingt (20) semaines à compter de la date de la signature du contrat.

X. PROFIL DU CABINET ET DES EXPERTS CLES

La mission sera confiée à une firme ou un consortium (le « Consultant ») ayant une compétence avérée et une expérience pertinente dans l'exécution réussie de missions similaires au profit de gouvernements dans des pays à revenus faibles et intermédiaires. Il est attendu que le Consultant démontre une forte capacité à exécuter la mission et à présenter un plan pour la conduire d'une manière inclusive et agile par rapport aux réalités locales et au contexte actuel. Il doit détailler dans sa proposition l'organisation logistique envisagée et le déploiement des compétences appropriées pour l'exécution de la mission.

La langue de travail orale et écrite sera le français.

Les critères d'évaluation en vue de la constitution de la liste restreinte sont :

- Être un cabinet de conseil ou un consortium multidisciplinaire spécialisé dans la gouvernance numérique, la cybersécurité / PKI et la transformation du secteur public.
- Minimum 10 ans d'activité dans les technologies de confiance numérique et l'e-Gouvernement.
- Au moins trois projets de portée nationale comportant la mise en place d'une infrastructure de signature électronique ou PKI, dont un en Afrique subsaharienne.
- Expérience en matière d'élaboration de stratégies ou feuilles de route pour la confiance numérique (e-ID, e-signature, services de confiance).
- Expérience en matière d'assistance législative ou réglementaire (rédaction de décrets, normes techniques, schémas de supervision).
- Expérience en matière de conception technique de solutions/services de confiance.
- Expérience en matière de modélisation financière et économique de services de confiance.
- Avoir une équipe pluridisciplinaire intégrée.
- Capacité à déployer des équipes bilingues français-anglais sur le terrain en RDC, avec un point focal local (bureau ou partenaire) pour la coordination logistique et le suivi post-mission.
- Avoir une expérience réussie en RDC serait un avantage.
- Expérience avérée des projets financés par des bailleurs (Banque mondiale, BAD, UE, etc.) serait un avantage.

Le consultant doit examiner attentivement l'étendue des travaux et proposer une équipe de personnel compétent et bien organisée pour exécuter la mission. Le chef de mission et les autres cadres de l'équipe de projet devront satisfaire aux exigences libellées dans le tableau 2 ci-dessous.

Tableau 2 : Profils des experts clés

Poste (personne-mois indicatif)	Responsabilités principales	Qualifications minimales	Atouts recherchés
1. Chef(fe) de mission / Team Leader (3 p-m)	• Conduite globale de l'étude, interface PATN/Banque mondiale. • Supervision qualité, arbitrage méthodologique, gestion des risques.	• Bac + 5 (Ingénierie, Informatique, Télécoms ou équivalent). • 10 ans d'expérience dont 5 comme chef(e) de projet e-Gouv ou PKI. • Certification PMP ou Prince2 Practitioner.	• Connaissance technique approfondie des meilleures pratiques en matière de gouvernance et des cadres techniques pour les e-signatures. Connaissance du contexte réglementaire OHADA et/ou du. • Pratique confirmée de la facilitation multi-acteurs.
2. Expert juridique & institutionnel (2 p-m)	• Analyse du cadre légal, rédaction des textes d'application. • Conseils sur la gouvernance ANCE / ARPTIC.	• Juriste (Bac + 5), spécialisation TIC ou droit des affaires. • 8 ans d'expérience, dont 3 sur e-signature ou protection des données. • Maîtrise des normes eIDAS / ETSI, droit OHADA.	• Connaissance technique approfondie des meilleures pratiques en matière de cadres juridiques et réglementaires pour les e-signatures. • Expérience en rédaction de projets de loi / des lignes directrices.

3. Architecte PKI / Expert technique e-Signature (2,5 p-m)	• Cartographie de l'existant, définition des scénarios d'architecture. • Développement de spécifications techniques, HSM (Hardware Security Module) certificate, politiques de certification (CP) / Déclaration de pratiques de Certification (CPS).	• Ingénieur ou MSc Sécurité (Bac + 5). • 10 ans dans le déploiement de PKI ou services de confiance. • Certifications CISSP ou CCSK, ISO 27001 Lead Implementer.	• Expérience dans l'analyse et le développement d'architectures et de spécifications techniques pour les e-signatures. • Expérience d'intégration avec plateformes gouvernementales (e-ID, e-procurement).
4. Expert cybersécurité & conformité (1,5 p-m)	• Analyse des menaces, plan de mitigation, exigences ISO 27001/27701. • Définition du dispositif d'audit et de supervision ANCE.	• Bac + 5 Sécurité informatique. • 8 ans d'expérience dont 3 en audits PKI. • Certifié CISA, ISO 27001 Lead Auditor ou équivalent.	• Connaissances techniques en matière de gestion des risques et d'audit. • Expérience NIST CSF, conception de Plan de Reprise des Activités (PRA)/Plan de Continuité des Activités (PCA) dans l'administration publique.
5. Économiste / Analyste financier (1,5 p-m)	• Modélisation CAPEX/OPEX, plan de financement. • Analyse coût-bénéfice et soutenabilité budgétaire.	• Bac + 5 Économie, Finance, MBA. • 8 ans sur business modelling ICT. • Connaissance des schémas de partenariats public-privé.	• Familiarité avec les mécanismes IDA
6. Spécialiste renforcement des capacités & communication (1 p-m)	• Élaboration du plan de formation, contenus e-learning. • Stratégie de sensibilisation multicanal (administrations, citoyens, secteur privé).	• Bac + 4 en communication ou sciences sociales. • 7 ans sur projets de changement organisationnel.	• Expérience dans la gestion de communication stratégique. • Expérience en design pédagogique numérique et inclusion de genre.

7. Expert suivi-évaluation (M&E) (0,5 p-m)	• Conception du cadre logique, KPI, mécanismes de reporting. • Appui à la mise en place d'outils de collecte.	• Bac + 4 Statistiques, Économie ou équivalent. • 5 ans en M&E de projets TIC ou gouvernance.	• Maîtrise d'outils digitaux de data-collection (KoboToolbox, ODK).
8. Coordinateur/trice national(e) (0,5 p-m)	• Liaison logistique, collecte de données locales. • Support continue aux missions terrain.	• Bac + 3 minimum. • 5 ans dans la coordination de projets IT en RDC. • Bilingue.	• Réseau établi avec les parties prenantes (administrations, citoyens, secteur privé, etc.).

Les personnes-mois (p-m) sont indicatifs et pourront être ajustés lors de la proposition technique.