



REPUBLIQUE DU SENEGAL

Un Peuple – Un But – Une Foi

.....

MINISTÈRE DE LA COMMUNICATION, DES TÉLÉCOMMUNICATIONS ET NUMÉRIQUE

.....



PROJET D'ACCELERATION DE L'ECONOMIE NUMERIQUE AU SENEGAL PAENS

Termes de références pour la mise en place d'une architecture d'entreprise gouvernementale et d'une étude de faisabilité sur la mise en place de l'identification numérique et de l'interopérabilité des plateformes, pour l'État du Sénégal.

NOVEMBRE 2023

Table des matières

1	Contexte	3
2	Objectifs	4
2.1	Objectif général	5
2.2	Objectifs spécifiques	5
2.3	Concepts détaillés	7
2.3.1	Écosystème d'identification numérique	7
2.3.2	Définition du cadre d'interopérabilité	8
2.3.3	Renforcement des systèmes existants d'identification de base	9
3	Étendue des travaux	10
3.1	Résumé	10
3.2	Périmètre détaillé	11
3.2.1	Consultations des parties prenantes et analyse des cas d'utilisation	11
3.2.2	Évaluation des dimensions juridiques, institutionnelles, stratégiques et technologiques ...	11
3.2.3	Options de conception et évaluation de la viabilité	12
3.2.4	Identification et atténuation des risques	13
3.2.5	Feuille de route pour la mise en œuvre	14
4	Durée de la mission et livrables	15
4.1	Durée de la mission	15
4.2	Livrables	15
5	Qualifications du consultant	16

1 CONTEXTE

La République du Sénégal, sous l'égide de son gouvernement, a entrepris des efforts et lancé d'importantes initiatives pour moderniser et numériser son administration publique afin d'améliorer la prestation de services publics. L'objectif est de réaliser cette transformation d'ici 2035 - conformément au Plan Sénégal Emergent - en mettant l'accent sur les services en ligne entre le gouvernement et les citoyens (G2P) et entre le gouvernement et les entreprises (G2B). Ces priorités sont inscrites dans le cadre de la Stratégie Sénégal Numérique 2025 et de la feuille de route de l'e-gouvernement, élaborées par le Gouvernement du Sénégal en 2021.

Le pivot central de cette stratégie E-gouvernement est la création d'une Administration publique qui soit à la fois numérique, intelligente et innovante, capable de servir les citoyens et les entreprises en ligne d'ici 2025.

En l'état, les systèmes d'informations de l'Administration sont caractérisés par leurs fragmentations, l'absence de redondance des données et de coordination, la prévalence des systèmes manuels mais aussi l'absence d'automatisation. Pour pallier ces problèmes, l'État du Sénégal, à travers les projets de Digitalisation confiés à Sénégal Numérique SA, promeut l'interopérabilité de Systèmes d'information de toute l'Administration (G2G). Une des étapes importantes mais souvent délaissée est l'approche d'une architecture d'entreprise gouvernementale (AEG), associée à la mise en place d'un écosystème d'identité numérique sécurisé et d'interopérabilité des plateformes e. Cela vise à soutenir la prestation de services publics numériques axés sur les citoyens, en permettant une identification et une authentification fiables lors des transactions numériques.

L'Architecture d'Entreprise est une méthodologie qui a pour finalité d'aligner les systèmes d'information sur la mission, les buts et les objectifs de différentes entités. En effet, elle permet d'établir une description schématique dans le but de mieux expliquer comment les différentes composantes devront communiquer.

Il existe plusieurs systèmes d'informations avec des rôles spécifiques. L'AEG permettra d'obtenir :

- Une cartographie des différents systèmes existants et leur alignement vers une architecture cible en faisant la représentation avec un cadre de référence, tel que l'Open Group Architectural Framework - TOGAF ;
- L'alignement des services publics et l'agilité digitale ;
- La gouvernance des décisions et les orientations digitales.

Dans le contexte de l'identité numérique, le Ministère en charge du Numérique a initié une étude de faisabilité préliminaire pour évaluer la possibilité et les options de conception potentielles pour un système d'identité numérique, dont les résultats sont disponibles. Le système envisagé permettra l'authentification numérique pour diverses transactions, y compris les interactions à distance ou en ligne, et complétera les systèmes d'identification existants, en se basant sur les fondamentaux techniques et juridiques.

Cependant, la mise en place d'un tel système ne s'arrête pas à la conception technique de la plateforme d'identité de base. En effet, plusieurs autres éléments constitutifs, y compris des cadres

juridiques et réglementaires appropriés et des arrangements institutionnels solides, seront nécessaires pour faciliter son fonctionnement et assurer sa viabilité à long terme.

L'objectif de la prestation décrite ci-après est d'une part i) la mise en place une architecture d'entreprise gouvernementale, pour l'État du Sénégal et d'autre part ii) la réalisation d'une étude de faisabilité sur la mise en place de l'identification numérique, de l'interopérabilité des plateformes et de la signature électronique, pour l'État du Sénégal. Cette seconde activité s'appuiera sur les Principes d'Identification pour le Développement Durable de l'ID4D (« Identification for Development ») et cherchera à s'aligner sur ceux-ci.

2 OBJECTIFS

Le système d'information Gouvernemental de l'État du Sénégal, dans sa globalité, est composé de multiples applications diverses dont le périmètre varie selon le secteur d'activité. Il est mis en œuvre par toutes les structures disposant de systèmes à fort impact. Il s'agit, entre autres :

- Agence de Couverture Maladie Universelle (ACMU) : SunuCMU
- Ministère chargé Fonction Publique : demande de recrutement dans la fonction publique
- Ministère des Finances et du Budget
 - o Système Intégré de Gestion de l'Information Financière SIGIFI
 - o Solde (eSolde)
 - o Direction Générale des Douanes (Orbus)
 - o Direction Générale des Impôts et Domaines (etax, SIGTAS)
 - o Direction Générale de la Comptabilité Publique et du Trésor (ASTER)
 - o Agence Nationale de Statistique et de la Démographie (NINEAWEB)
- Ministère de l'Intérieur
 - o Direction de l'Automatisation du Fichier (carte d'identité biométrique)
 - o Direction de la Police des Etrangers et des Titres de Voyages DPETV (passeport biométrique)
- Ministère des Forces Armées : SIGRH
- Ministère de l'Education Nationale : MIRADOR
- APIX SA : Guichet création des entreprises
- Ministère de la Justice : Registre du Commerce et du Crédit Mobilier (RCCM)
- Sénégal Numérique SA
 - o SIGRNU/PNSBF (Délégation Générale de la Protection Sociale et de la Solidarité Nationale) : bourse de sécurité familiale,
 - o Guichet unique/TeleDac : portail des procédures dématérialisées de l'administration,
 - o Gestion Intégrée des Ressources et Agents administration et des GIRAFE (Fonction Publique) : Gestion des Actes d'administration des Agents de l'Etat.

L'environnement technologique actuel du système d'information de l'État est hétérogène, plusieurs cas de figures sont à noter dans la mise en place des applications peut passer par :

- Le développement « from » scratch avec des langages de programmation tels que le J2EE, PHP, C++, ou avec des framework comme laravel, symphony etc.,
- L'acquisition de logiciels clés en main, propriétaire, auprès de constructeur,

- La customisation de logiciel open source,
- La mise en place de base de données avec mysql server, oracle etc.

La liste ci-dessus, non exhaustive, donne une idée générale du SI de l'Etat du Sénégal.

2.1 OBJECTIF GENERAL

L'objectif général est de mettre en place une Architecture d'Entreprise Gouvernementale (AEG) et réaliser une étude de faisabilité sur la mise en place de l'identification numérique et de l'interopérabilité des plateformes, pour l'État du Sénégal.

2.2 OBJECTIFS SPECIFIQUES

De manière spécifique, les objectifs de cette mission sont de :

- **Proposer une AEG complète pour l'ensemble du Gouvernement.** Le soumissionnaire tiendra compte du paysage technologique actuel ainsi que des exigences futures. L'architecture proposée devra contenir un schéma directeur pour une approche stratégique de l'ensemble de l'Administration, en tenant compte des personnes, des processus et des éléments technologiques. L'architecture devra être évolutive, adaptable et alignée sur les stratégies pertinentes
 - Faire un audit exhaustif du SI de l'État du Sénégal ;
 - Mettre en place d'un schéma directeur pour toute l'Administration ;
 - Faire un alignement sur la stratégie numérique globale de l'Administration ;
 - Proposer 2 cas d'utilisation d'application de l'AEG pour l'État du Sénégal, dont un relatif au domaine de la santé ;
 - Définir une architecture d'entreprise gouvernementale solide avec des stratégies d'interopérabilité pour permettre aux différents SI sectoriels de l'Administration d'être interopérables, d'échanger des données, mais aussi de permettre à l'Administration d'améliorer l'efficacité de ses opérations, de réduire les redondances, d'effectuer des échanges optimisés de données, de fournir une meilleure qualité des services publics et de faciliter la prise de décision ;
 - Sécurité et protection des données à caractère personnel compte tenu des bonnes pratiques internationales mais aussi de la loi Sénégalaise portant sur la protection des données à caractère personnel, et son décret d'application, qui ont pour objet de garantir le respect des droits fondamentaux des particuliers dans le cadre du traitement des données à caractère personnel intégrer dans l'architecture d'entreprise gouvernementale des mesures de sécurité et protection des données dès la conception et par défaut, robustes et accessibles.
 - Proposer une stratégie d'atténuation des effets et adaptation au réchauffement climatique, tenant compte des matériels à acquérir et déployer entre autres.
 - Adoption du numérique : élaborer des stratégies sectorielles visant à promouvoir la valeur et les avantages des services numériques auprès du public, et de concevoir

- l'architecture en mettant l'accent sur la facilité d'utilisation afin d'encourager l'adoption de ces services.
- Conception centrée sur l'utilisateur : définir une architecture d'entreprise gouvernementale facilitant la fourniture de services centrés sur l'utilisateur, pour permettre des interactions faciles, efficaces et personnalisées entre le Gouvernement et ses citoyens ;
 - Normalisation : Normaliser l'utilisation de technologies, de protocoles et de formats de données pour garantir la compatibilité, réduire la complexité et faciliter l'intégration dans l'ensemble de l'écosystème gouvernemental ;
 - Évolutivité et flexibilité : définir une architecture d'entreprise gouvernementale qui doit être évolutive et flexible pour s'adapter aux changements dans les services gouvernementaux, les orientations politiques et les avancées technologiques ;
 - Capacité et compétences : Concevoir une architecture d'entreprise gouvernementale qui tiendra en compte des compétences et de la capacité des administrations à mettre en œuvre, gérer et faire évoluer l'architecture au fil du temps ;
 - Contraintes d'infrastructures : Adapter l'architecture d'entreprise gouvernementale conçue pour fonctionner efficacement avec des contraintes telles qu'une infrastructure informatique existante limitée ;
 - Contexte local : définir une architecture d'entreprise gouvernementale qui prendra en compte les contextes socioculturels, économiques et géographiques spécifiques du Sénégal ;
 - Gouvernance : Définir une structure de gouvernance solide pour gérer et guider le développement et le fonctionnement de l'architecture d'entreprise, en veillant à ce qu'elle continue à s'aligner avec les objectifs stratégiques et à apporter de la valeur.
- **Réaliser une étude de faisabilité sur la mise en place de l'identification numérique et de l'interopérabilité des plateformes :**
- Réaliser une étude détaillée sur la mise en place de l'identification numérique au niveau national, en tenant compte de l'étude de faisabilité préliminaire sur une identité numérique nationale (INN) initiée par le Ministère en charge du Numérique et les bonnes pratiques internationales, dont l'alignement avec les Principes sur l'identification pour un développement durable et les concepts détaillés dans la section 2.3.1 ;
 - Étudier et définir un cadre d'interopérabilité entre les systèmes, les bases de données et les services numériques de l'Administration ;
 - Réaliser une analyse approfondie de tous les systèmes d'identification actuels, tels que le système national d'identification, le système d'enregistrement des faits d'état civil, pour ne citer que cela, en tenant compte des efforts de numérisation passés et en cours, afin d'identifier les lacunes et de proposer une feuille de route pour un renforcement continu et une synergie en vue de leur permettre d'étayer le développement de l'économie numérique.

2.3 CONCEPTS DETAILLES

2.3.1 Écosystème d'identification numérique

- **Fonctionnalité** : L'écosystème de l'identité numérique devrait inclure des fonctionnalités essentielles de l'identité numérique, considérées comme pertinentes pour les cas d'utilisation identifiés et hiérarchisés, telles que la confirmation de la validité des titres, l'authentification numérique forte de l'identité des personnes et la vérification des attributs à partir de sources faisant autorité.
- **Interopérabilité** : Le système d'identification numérique doit être conçu pour être interopérable avec d'autres systèmes, bases de données et services numériques, tant à l'intérieur qu'à l'extérieur du secteur public. Cela nécessite l'adoption de normes ouvertes, d'API et de protocoles d'échange de données.
- **Conception centrée sur l'utilisateur** : L'écosystème de l'identification numérique doit être conçu selon une approche centrée sur l'utilisateur. Le système doit être facile à utiliser et accessible à tous, quelles que soient leurs compétences techniques. Les besoins des utilisateurs, leurs habitudes et les obstacles potentiels à l'utilisation (tels que la langue, le revenu, la culture numérique, le handicap, le sexe, l'âge, etc.
- **Accessibilité et inclusion** : Le système doit être conçu pour atteindre et satisfaire tous les groupes démographiques, y compris ceux qui n'ont pas accès à l'internet ou à des appareils numériques, les populations rurales, les personnes handicapées, les personnes âgées et d'autres groupes vulnérables. Il convient en particulier de planifier l'enregistrement et la délivrance des titres, ainsi que l'adoption de mécanismes de vérification et d'authentification de l'identité numérique. La conception de l'inclusion pourrait impliquer des approches variées ou différenciées pour les différentes populations cibles, en donnant de multiples moyens d'accès et d'utilisation des identités numériques, par exemple via des appareils mobiles ou des services d'assistance dans des centres communautaires locaux.
- **Protection des données à caractère personnel et cybersécurité** : le Sénégal a adopté la loi n°2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel, et son décret d'application, qui ont pour objet de garantir le respect des droits fondamentaux des particuliers dans le cadre du traitement des données à caractère personnel, et procède actuellement à la modernisation de ce cadre pour tenir compte de l'évolution des bonnes pratiques internationales et des capacités nationales en la matière. La protection de la vie privée et la sécurité doivent être au cœur de la conception de l'écosystème de la carte d'identité numérique. Il s'agit notamment de protéger les données personnelles et d'adhérer aux principes de minimisation des données et de limitation des finalités. En guise d'illustration, il faudra pouvoir limiter la communication d'informations aux seules données essentielles, aux seules parties qui les nécessitent. La sécurité de cette identité numérique permettrait qu'elle ne soit pas « fraudable », permettrait de protéger contre le traçage des transactions et contre la divulgation des données communiquées. Des mesures efficaces de protection de la vie privée dès la conception, y compris le cryptage des données et des protocoles de communication sécurisés, devraient être intégrées dans la conception du système. Ces éléments doivent être inscrits dès la conception et par défaut dans un système d'identification numérique, en passant par le cadre légal et réglementaire, la gouvernance et la structure organisationnelle du système d'identification, ainsi que dans

l'architecture du système elle-même, et être associée à un cadre de suivi et évaluation robuste.

- **Autonomisation de l'utilisateur** : Les fonctions de responsabilisation de l'utilisateur doivent être intégrées par défaut. Il pourrait s'agir, par exemple, de privilégier les confirmations oui/non sur le partage des attributs d'identité, d'exiger le consentement pour certaines transactions, de fournir une piste d'audit transparente des transactions d'identité numérique et de permettre aux utilisateurs de divulguer sélectivement des attributs aux parties qui se fient à eux, de disposer d'un objet personnel comme support l'identité numérique qui permettrait de présenter son identité numérique quand et uniquement c'est voulu
- **Neutralité technologique et innovation** : La conception doit être neutre sur le plan technologique et permettre l'intégration de technologies et de normes émergentes telles que les portefeuilles d'identité mobiles et les justificatifs vérifiables, tout en étant adaptable pour suivre le rythme des technologies d'authentification nouvelles et en constante évolution. L'écosystème de l'identité doit rester adaptable et capable d'intégrer les progrès des technologies de l'identité au fur et à mesure de leur apparition.
- **Participation du secteur privé** : La conception du système d'identification numérique devrait permettre aux entités du secteur privé de participer en tant que fournisseurs d'identité, y compris par le biais d'architectures fédérées. Cela pourrait impliquer l'adoption d'une approche de normes ouvertes et la création d'un cadre qui soutienne diverses solutions d'identité, ce qui pourrait conduire à une augmentation de l'innovation et de la compétitivité.

2.3.2 Définition du cadre d'interopérabilité

- **Normes de données communes** : Il est essentiel d'établir des normes de données communes à l'ensemble de l'Administration pour les données qui seront échangées à grande échelle, afin de garantir que les données provenant de différentes sources puissent être comprises et utilisées de manière cohérente. Le cabinet devra identifier les cas d'utilisation prioritaires pour le partage des données, classer par ordre de priorité les types de données (privées, publiques...) pour lesquels une normalisation au niveau de l'ensemble de l'Administration est appropriée. Ces normes devraient être alignées sur les pratiques internationales, le cas échéant, devront définir les standards à respecter, afin de faciliter la gestion des données et l'échange de données avec l'extérieur. Ces normes une fois mise en place, à travers une loi ou un acte réglementaire où tout autre mécanisme garantissant sa pérennité, permettront précisément
- **Sécurité** : Il est fondamental de garantir la sécurité des échanges de données. Le cadre d'interopérabilité doit garantir que les meilleures pratiques et standards internationaux en matière de sécurité de l'information sont appliquées avant, pendant et après l'échange de données. Le Sénégal ayant voté une loi sur la cybersécurité ... Les parties recevant des données par l'intermédiaire du cadre d'interopérabilité devraient disposer des éléments suivants
- **Protection des données à caractère personnel** : Le cadre doit comprendre des politiques et des mécanismes clairs de protection des données, y compris des techniques d'anonymisation si nécessaire, et adhérer aux lois nationales sur la protection des données

et aux bonnes pratiques internationales. En effet, le Sénégal a voté la loi n°2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel, et son décret d'application, en cours de mise à jour, qui ont pour objet de garantir le respect des droits fondamentaux des particuliers dans le cadre du traitement des données à caractère personnel. Les exemples incluent des contrôles d'accès stricts, des règles d'entreprise pour l'autorisation, une piste d'audit vérifiable de toutes les activités de partage de données, ainsi que la transparence pour les individus sur quand et avec qui leurs données sont partagées.

- **Gouvernance et gestion** : Des structures claires de gouvernance et de gestion doivent être établies pour superviser les activités de partage des données, gérer les litiges et garantir le respect des politiques et des normes. Les rôles et les responsabilités des différents acteurs devront être clarifiés, avec la prise d'actes réglementaires, le cas échéant.
- **Contraintes d'infrastructure** : Étant donné que l'infrastructure informatique existante est limitée, la conception de l'architecture doit être adaptée pour fonctionner efficacement dans le cadre de ces contraintes. Des solutions basées sur l'informatique en nuage pourraient être envisagées le cas échéant. Les solutions proposées doivent éviter, dans la mesure du possible, les cas de dépendances fortes aux fournisseurs et de « legacy systems ».
- **Confiance du public** : La transparence des pratiques de partage des données peut contribuer à renforcer la confiance du public. Il s'agit notamment de communiquer clairement sur les données partagées, avec qui et dans quel but. Le fait d'exiger le consentement le cas échéant et de mettre en place des systèmes permettant de vérifier le consentement donné, notamment par l'authentification de l'identité numérique, peut contribuer à renforcer la confiance du public.

2.3.3 Renforcement des systèmes existants d'identification de base

- **État de la numérisation** : Évaluer l'état actuel de la numérisation des systèmes d'identification de base, y compris le registre civil et les systèmes d'identification nationaux. Il s'agirait de comprendre la nature des données qui sont actuellement numérisées, les données qui sont encore sous forme physique et l'infrastructure existante pour le stockage et l'extraction des données.
- **Initiatives de transformation numérique** : Examiner les efforts actuels et passés pour numériser ces systèmes. L'objectif est de comprendre les facteurs de réussite, les défis et les résultats afin d'éclairer les initiatives futures. Cet examen devrait également porter sur les enseignements tirés et la manière dont ils peuvent être appliqués pour garantir que ces systèmes sont prêts à soutenir l'écosystème de l'identification numérique.
- **Interopérabilité et normalisation** : Évaluer le niveau actuel d'interopérabilité et de normalisation de ces systèmes. Il s'agit notamment de déterminer s'ils sont conçus pour s'interfacer avec d'autres systèmes et s'ils adhèrent à des normes internationalement reconnues qui faciliteraient cette interopérabilité. Des solutions devront être proposées pour parvenir à l'interfaçage des systèmes et l'échange de données normalisés.
- **Préparation à l'intégration** : Évaluer l'aptitude de ces systèmes à s'intégrer dans l'économie numérique. Il s'agit d'évaluer la capacité de l'infrastructure actuelle à supporter l'augmentation des volumes de transactions, la robustesse de ses systèmes de sécurité et sa capacité à s'adapter à l'évolution des besoins des utilisateurs.

- **Accessibilité et inclusion** : Évaluer le degré d'accessibilité et d'inclusivité de ces systèmes. Il s'agit de comprendre les éventuels obstacles à l'accès et les stratégies qui pourraient être utilisées pour surmonter ces obstacles.

3 ÉTENDUE DES TRAVAUX

Pour chacun des volets de l'étude, objet de ces TDR, (écosystème d'identification numérique, interopérabilité et partage des données, et renforcement des systèmes d'identification de base existants), le cabinet de conseil doit prendre en compte les aspects ci-dessous.

3.1 RESUME

Avec une analyse et des recommandations distinctes et détaillées, tout en assurant la cohérence stratégique et technique entre les systèmes.

1. Cartographie des parties prenantes. Le cabinet de conseil doit identifier les principales parties prenantes multipartites, notamment les agences gouvernementales, les entités du secteur privé, les organisations non gouvernementales/ de la société civile, le secteur académique et les citoyens, en incluant les populations vulnérables. Pour chaque partie prenante identifiée, le cabinet de conseil doit dresser la carte de son rôle, de ses intérêts, de son influence et de son impact potentiel sur le projet.
2. Consultations des parties prenantes : Le cabinet de conseil doit mener des consultations approfondies avec les parties prenantes identifiées, afin de recueillir des informations et de comprendre, documenter et hiérarchiser les cas d'utilisation pour les différentes composantes du projet. Ces consultations doivent constituer la base d'un engagement et d'une consultation significatifs tout au long du projet, en garantissant une approche participative qui tienne compte de divers points de vue et favorise l'adhésion.
3. Évaluation technique des dimensions juridiques, institutionnelles, stratégiques et technologiques : Le cabinet de conseil devra évaluer de manière exhaustive les différentes dimensions du projet. Il s'agira notamment d'examiner l'environnement juridique et réglementaire, les structures institutionnelles et de gouvernance, les objectifs stratégiques, ainsi que les prérequis technologiques et l'infrastructure publique numérique nécessaires pour soutenir la mise en œuvre. L'évaluation technique devra faire des propositions intégrant les normes et standards internationaux liés à chacun des secteurs qui sera étudié. Le consultant devra se familiariser avec et tenir compte d'études existantes, de résultats des consultations avec des parties prenantes sur le sujet, et autres sources de documentation pertinente pour s'assurer de la complémentarité de ses recommandations.
4. Options de conception et évaluation de la viabilité : Une fois l'étude de faisabilité achevée, le cabinet de conseil devra proposer plusieurs options pour les modèles de mise en œuvre des différentes composantes du projet, compte tenu du secteur privé, afin de permettre au gouvernement du Sénégal de prendre une décision éclairée sur la voie la plus appropriée à suivre.
5. Identification et atténuation des risques : Le cabinet de consultants devra identifier les risques potentiels, les dépendances, les opportunités et les défis qui peuvent survenir dans la mise en œuvre du projet, et suggérer des mesures d'atténuation pratiques et efficaces.

6. Feuille de route pour la mise en œuvre : Sur la base des résultats des tâches ci-dessus, le cabinet de conseil devra élaborer une feuille de route détaillée pour la mise en œuvre de l'écosystème de l'identification numérique et au moins 3 scénarii de mise en œuvre, en faisant ressortir les atouts et inconvénients, le cas échéant. Cette feuille de route devrait décrire, la meilleure orientation, la séquence des activités, les calendriers, les responsabilités, les estimations de coûts et les indicateurs de performance.

3.2 PERIMETRE DETAILLE

3.2.1 Consultations des parties prenantes et analyse des cas d'utilisation

- Consultations des parties prenantes : Mener des consultations avec les agences gouvernementales concernées, les entités du secteur privé, les organisations de la société civile, les prestataires de services et les parties utilisatrices, ainsi que les particuliers, et définir les cas d'utilisation prioritaires et les besoins des utilisateurs.
- Analyse des cas d'utilisation : L'analyse des cas d'utilisation impliquera de documenter les différents types de transactions numériques et en ligne qui devraient être facilitées par ce système, ainsi que les exigences et les défis spécifiques associés à chacun d'entre eux.
- Établissement de priorités : L'impact élevé doit être analysé en termes de potentiel de développement de l'économie numérique, de réduction de la pauvreté, d'amélioration de la prestation de services et d'amélioration de la transparence et de la responsabilité. D'autres considérations incluent la rentabilité, la facilité d'utilisation, les économies fiscales, la viabilité financière et opérationnelle et l'acceptation par les utilisateurs.
- Documentation : La documentation et les recommandations relatives aux cas d'utilisation doivent être communiquées dans un langage clair et simple afin de faciliter la compréhension des avantages potentiels par les parties prenantes, en particulier si les nouveaux processus s'écartent des pratiques existantes.

3.2.2 Évaluation des dimensions juridiques, institutionnelles, stratégiques et technologiques

- Évaluation stratégique : Le cabinet de conseil doit évaluer la manière dont les initiatives proposées s'alignent sur les objectifs stratégiques plus larges décrits dans le Plan Sénégal Emergent (PSE), la Stratégie Sénégal Numérique (SN2025), la stratégie e-Gouvernement (eGov), et d'autres stratégies nationales et sectorielles pertinentes. Il s'agit notamment de comprendre comment ces initiatives contribuent à la vision stratégique globale, comment elles se recoupent avec d'autres initiatives mises en œuvre dans ce cadre stratégique et comment elles peuvent être intégrées dans la planification stratégique globale et le cadre de suivi.
- Analyse des tendances et des meilleures pratiques : Le cabinet de conseil doit examiner et analyser la pertinence des tendances, des normes et des bonnes pratiques actuelles. Il s'agit notamment des tendances en matière d'adoption des technologies, de comportement des utilisateurs, d'évolution de la réglementation et de solutions innovantes. La compréhension de ces tendances permettra de s'assurer que les initiatives proposées sont à l'épreuve du temps et adaptables à l'évolution des circonstances. Il convient également d'analyser les normes et les cadres internationaux et nationaux existants qui sont pertinents pour les

initiatives proposées. D'autres bonnes pratiques doivent être évaluées, telles que les structures de gouvernance, les processus d'engagement des parties prenantes et les approches de gestion des risques.

- **Évaluation juridique :** Le cabinet de conseil doit procéder à un examen du cadre juridique relatif à l'administration numérique, dans sa totalité. Il s'agit notamment de comprendre les lois, réglementations et normes existantes, d'identifier les lacunes et les incohérences, et de recommander les changements ou la nouvelle législation nécessaires pour soutenir l'écosystème numérique. Ce travail sera effectué en étroite coordination avec le MCTN et le cabinet juridique qui soutiendra le ministère avec une assistance technique sur l'environnement juridique et réglementaire lié à l'économie numérique au Sénégal.
- **Évaluation institutionnelle :** Le consultant doit examiner les structures institutionnelles existantes qui sont pertinentes pour les initiatives proposées, y compris leurs rôles, leurs responsabilités, leurs capacités et leurs interrelations. Cet examen devrait permettre d'identifier les lacunes ou les goulots d'étranglement institutionnels susceptibles d'entraver la mise en œuvre des initiatives et de suggérer des solutions possibles. Elle devrait également envisager la nécessité de créer de nouvelles institutions, telles qu'une agence spécialisée dans la gestion du système d'identification numérique, et définir leurs rôles et structures potentiels.
- **Évaluation des technologies actuelles :** Le cabinet doit procéder à un examen approfondi du paysage technologique en rapport avec les initiatives proposées. Il s'agit notamment de comprendre l'état actuel des infrastructures numériques au Sénégal, les options technologiques disponibles ainsi que leur adéquation au contexte local. L'évaluation devrait également prendre en compte les questions de sécurité technologique, de résilience, d'accessibilité et de convivialité.

Recommandations : Sur la base de l'analyse des tendances, des meilleures pratiques et des normes, le cabinet de conseil doit fournir des recommandations sur la manière dont ces informations peuvent être intégrées dans la conception et la mise en œuvre des initiatives proposées. Ces recommandations doivent viser à améliorer l'efficacité, l'efficience, la durabilité et la convivialité de ces initiatives, et à garantir leur conformité aux normes internationales et leur compatibilité avec les systèmes mondiaux.

3.2.3 Options de conception et évaluation de la viabilité

- **Menu d'options de conception :** Effectuer une analyse complète des options de conception potentielles. Il s'agit de comparer et d'opposer différentes architectures, modèles de mise en œuvre, exigences en matière d'infrastructure, processus opérationnels et mesures de sécurité. Chaque option de conception doit être sélectionnée de manière stratégique pour offrir des visions alternatives de la manière dont les cas d'utilisation et les exigences peuvent être satisfaits grâce à différentes stratégies de mise en œuvre.
- **Analyse technique :** le cabinet doit évaluer les exigences techniques nécessaires à la mise en œuvre des initiatives proposées. Des facteurs tels que l'infrastructure technologique disponible, l'expertise technique requise, l'intégration avec les systèmes existants, les exigences en matière de sécurité et l'intégration avec les systèmes existants. L'analyse de l'intégration doit porter sur les ressources humaines, les processus et les éléments technologiques, et doit comprendre une analyse technique des systèmes actuels, de leurs capacités et de leurs limites, ainsi que des exigences relatives à leur mise à niveau ou à leur

interconnexion avec les options de conception proposées. Cette analyse technique fera ressortir une cartographie exhaustive des SI de l'État ainsi qu'une classification fine et détaillée des données, qui devraient être échangées entre les différents systèmes.

- Participation du secteur privé. L'étude devrait explorer les options et les modèles de participation du secteur privé à la mise en œuvre. Il pourrait s'agir de fournir certains services, de développer ou de gérer des parties de l'infrastructure, ou de jouer d'autres rôles. Les avantages et les risques d'une telle participation, ainsi que les cadres réglementaires et opérationnels nécessaires pour la faciliter, doivent être examinés.
- Évaluation des coûts et de la viabilité. Ces options devraient être chiffrées, comparées et évaluées sur la base de différents critères, notamment l'impact sur le développement de l'économie numérique, la pertinence stratégique, la faisabilité juridique et institutionnelle, la faisabilité technique, la rentabilité et les implications budgétaires, la viabilité financière et opérationnelle, l'adéquation aux besoins compte tenu des cas d'utilisation identifiés, l'acceptation socioculturelle, l'extensibilité, l'adaptabilité, l'accessibilité et la convivialité, l'impact potentiel sur la vie privée et la sécurité, ainsi que d'autres critères.
- Analyse de durabilité : Le cabinet évaluera la viabilité à long terme des initiatives proposées, en tenant compte de facteurs tels que les sources de financement, le recouvrement des coûts, l'évolutivité, l'adaptabilité aux changements futurs, l'absence de verrouillage des fournisseurs et des technologies, et la capacité d'amélioration continue. L'analyse doit être effectuée en vue d'encourager un écosystème gouvernemental et commercial durable qui inciterait les fournisseurs de services et les parties utilisatrices à créer et à utiliser des services sur la base des besoins des utilisateurs identifiés et des cas d'utilisation prioritaires.

3.2.4 Identification et atténuation des risques

- Identification des risques : Le cabinet procédera à une identification approfondie des risques et des dépendances associées à chaque composante du projet, dans divers domaines tels que technique, juridique, institutionnel, social, financier et opérationnel. Cela comprend, par exemple, les défaillances technologiques, les changements réglementaires, les goulots d'étranglement institutionnels, la résistance des parties prenantes, les dépassements de coûts, les compétences numériques, la connectivité dans les zones rurales et les conditions préalables juridiques et institutionnelles et les risques d'exclusion pour s'assurer d'une approche centrée sur l'utilisateur.
- Analyse des risques : Les risques doivent être analysés en termes d'impact potentiel et de probabilité d'occurrence. Cette analyse doit prendre en compte à la fois les conséquences directes du risque (telles que les retards, l'augmentation des coûts ou les réactions négatives du public) et les effets potentiels indirects ou à long terme (tels que l'atteinte à la réputation, la perte de confiance ou les occasions manquées). Les risques doivent être classés par ordre de priorité en fonction de leur impact potentiel et de leur probabilité afin de concentrer les efforts d'atténuation des risques sur les risques les plus importants.
- Atténuation des risques. Pour chaque risque identifié et hiérarchisé, le cabinet doit élaborer une stratégie d'atténuation. Cette stratégie doit décrire les mesures visant à empêcher le risque de se produire, à réduire sa probabilité ou son impact, ou à gérer ses conséquences s'il se produit. Les stratégies d'atténuation peuvent inclure, par exemple, des plans

d'urgence, des solutions alternatives, des ressources supplémentaires ou des activités d'engagement des parties prenantes.

- Plan de gestion des risques : Les résultats des activités d'identification, d'analyse, de hiérarchisation, d'atténuation et de suivi des risques doivent être compilés dans un plan global de gestion des risques. Ce plan devrait servir de guide pratique pour la gestion des risques tout au long de la mise en œuvre des initiatives proposées.

3.2.5 Feuille de route pour la mise en œuvre

- Benchmark : Le cabinet devra proposer une étude benchmark sur la mise en place d'une Identité numérique dans 4 pays, tenant compte du contexte technologique, social, ... du Sénégal, en sus de l'utilisation de bonnes pratiques et standards/normes internationaux.
- Cadre de planification : Le cabinet doit établir un cadre de planification clair et détaillé décrivant les principales étapes, activités, responsabilités, échéances et ressources nécessaires à la mise en œuvre de l'option ou des options de conception sélectionnée(s).
- Approche progressive : La feuille de route doit adopter une approche progressive qui permette de mettre en œuvre, de tester et d'étendre graduellement les initiatives. Cette approche devrait inclure des critères clairs pour passer d'une phase à l'autre, sur la base de la réalisation d'objectifs spécifiques et d'une gestion réussie des risques identifiés.
- Plan d'engagement des parties prenantes : Compte tenu de l'impact considérable des initiatives proposées, la feuille de route devrait comprendre un plan d'engagement des parties prenantes aux différents stades de la mise en œuvre. Ce plan doit identifier les principales parties prenantes, leurs rôles et leurs intérêts, les stratégies de participation et les mécanismes de communication et de retour d'information.
- Gestion du changement : La mise en œuvre des composantes du projet et leur intégration dans les systèmes et processus existants constituent une initiative de changement importante. Des processus efficaces de gestion du changement devront être mis en place pour garantir une adoption réussie. Les approches de conception modulaires et basées sur les composants permettront une mise en œuvre progressive adaptée aux contraintes de capacité.
- Interdépendances et coordination : La feuille de route devrait mettre en évidence les interdépendances entre les différentes activités et composantes des initiatives, et présenter des stratégies pour une coordination et une synchronisation efficace. Ceci est particulièrement important pour assurer un échange de données sans heurts entre les différentes bases de données et les différents systèmes.
- Possibilités en aval. Identifier les activités potentielles de mise en œuvre en aval qui pourraient être soutenues par un financement supplémentaire et/ou une coordination avec d'autres donateurs.

4 DUREE DE LA MISSION ET LIVRABLES

4.1 DUREE DE LA MISSION

La durée de la mission est prévue pour 12 mois et se déroulera sur le territoire sénégalais.

L'approche méthodologique devra comprendre les activités décrites ci-dessus et sera structurée principalement en 2 parties. La 1^{ère} phase concerne la mise en place de l'architecture d'entreprise gouvernementale, à l'issue de laquelle dans la 2^{ème} phase, il sera question de réaliser une étude de faisabilité sur la mise en œuvre de l'identification numérique et de l'interopérabilité des plateformes pour l'État du Sénégal.

4.2 LIVRABLES

Livrables clés		Calendrier	Jalon de paiement
Livable 1	Rapport de démarrage présentant la méthodologie des études, le plan d'action et le calendrier du consultant	3 semaines après avis de démarrage	10%
Livable 2	Cartographie des parties prenantes et rapport sur les consultations des parties prenantes,	8 semaines après avis de démarrage	10%
	Documentation des cas d'utilisation (AEG, INN, ...) avec hiérarchisation,		
	Rapport d'évaluation des cadres juridiques, institutionnels et stratégiques et du paysage technologique sur l'AEG, INN et interopérabilité.		
Livable 3	Options de conception et analyse de viabilité,	16 semaines après avis de démarrage	30%
	Vision architecturale définissant la cible en termes de capacités métiers, données, applicatives et technologiques,		
	Feuille de route budgétisée de mise en œuvre de l'architecture sur 3-5 ans,		
	Modèles de données décrivant les entités métiers et leurs relations,		
	Modèles d'interactions décrivant les échanges entre les différents systèmes internes et externes,		
	Cartographie exhaustive des applications existantes et cibles avec leurs interdépendances,		
	Cartographie technologique exhaustive des infrastructures et plateformes cibles		
Livable 4	Plan de gouvernance de l'architecture d'entreprise,	26 semaines après avis de démarrage	10%
	Plan de communication et de formation des parties prenantes,		
	Plan de gestion du changement pour accompagner l'adoption de la cible		

Livrable 5	Spécifications détaillées des interfaces techniques pour assurer l'interopérabilité (API, protocoles, standards, etc...),	40 semaines après avis de démarrage	20%
	Benchmark des standards et technologies d'identité numérique et d'interopérabilité pertinents (SAML, OpenID Connect, OAuth2, FIDO2, etc.),		
	Rapport détaillé d'interopérabilité entre les briques d'identification, d'authentification, les différents systèmes...		
	3 propositions d'architecture technique détaillée pour l'interopérabilité et l'identité numérique		
Livrable 6	Estimations budgétaires et identification des sources de financement,	45 semaines après avis de démarrage	10%
	Tableau de bord et indicateurs de suivi de la mise en œuvre et des bénéfices,		
	Analyse des risques et plan d'atténuation des risques,		
	Feuille de route pour le modèle de mise en œuvre sélectionné		
Livrable 7	Rapport final et recommandations Document de synthèse	49 semaines après avis de démarrage	10%

A la fin de la 1^{ère} phase, [X semaines après le démarrage] relative à la mise en place de l'AEG, un atelier de restitution des livrables sera organisé.

La version définitive pour chaque livrable sera transmise par le cabinet en version physique et électronique (Word, PDF, Excel et Power Point), une semaine (1) après les retours formulés par SENUM SA. Le paiement sera effectué après validation de la version définitive du livrable

5 QUALIFICATIONS DU CONSULTANT

Le cabinet de consultants (les membres du consortium et ses sous-traitants) doit posséder les compétences et l'expertise suivantes :

- Une expérience avérée dans la réalisation de missions similaires, en particulier dans la mise en place d'architecture d'entreprise gouvernementale et dans les missions d'études de faisabilité dans le domaine informatique (au moins 2 références de mise en place d'architecture d'entreprise gouvernementale) ;
- Expérience de travail dans les pays en développement et plus particulièrement en Afrique de l'Ouest, et connaissance du contexte social, culturel, politique et économique du Sénégal (2 références de missions organisationnelles dans des structure publiques) ;
- Connaissance avérée des normes internationales et des meilleures pratiques dans le domaine de l'économie numérique ;
- Expertise technique en matière d'identité numérique, d'interopérabilité, d'infrastructure des TIC, de sécurité numérique, de confidentialité et de protection des données, ainsi que dans des domaines connexes (au moins 1 référence de mise en place de système d'identification ou similaire) ;

- Expertise démontrée dans l'évaluation des cadres juridiques et institutionnels pour la transformation numérique ;
- Minimum de 2 références en tant que soumissionnaire principal ou chef de file de projet au profit de structures publiques d'un montant au moins égal à celui du présent marché.
- Aptitude avérée à dialoguer avec un large éventail de parties prenantes, des fonctionnaires aux utilisateurs finaux, dans le cadre d'un processus consultatif ;
- Maîtrise du français.

L'équipe doit posséder les compétences et l'expertise suivantes :

Profile	Expertise
Chef d'équipe / Chef de projet	• Au moins un master en systèmes d'information, en informatique ou dans un domaine connexe. • Au moins 8 ans d'expérience l'audit, la définition de stratégies sur les SI avec des certifications (COBIT, TOGAF, CISA, ...), dans la définition ou la mise en œuvre de stratégies numériques gouvernementales, dans la gestion de projets TIC complexes, en particulier dans les domaines pertinents pour cette mission. • Solides compétences en matière de systèmes d'information, de leadership et de communication.
Architecte d'entreprise	• Au moins un master en systèmes d'information, en informatique ou dans un domaine connexe. • Au moins 10 ans d'expérience dans la conception et la mise en œuvre de projets TIC à grande échelle. • Au moins 5 ans d'expérience dans la définition et la mise en œuvre d'architectures d'entreprise à l'échelle de l'administration. • Connaissance avérée des cadres et normes internationaux en matière d'architecture d'entreprise. • Certification : TOGAF, CISA, COBIT, PMP serait un atout
Expert réseaux et télécoms,	• Diplôme de niveau minimum bac+5 (généraliste, électronique, informatique, télécommunication) • Maîtrise parfaite de la langue française ; • Une expérience d'au moins 5 ans dans la mise en œuvre de réseaux informatiques complexes ; • Expérience de conception ou réalisation ou exploitation d'au moins un data center ; • Expérience dans les audits informatiques (réseau-systèmes-sécurité-applications) ; • Expérience dans l'entretien d'un réseau d'envergure nationale • Idéalement, expérience avec des administrations en Afrique ; • Certifications : CCNP, CCIE, etc. serait un atout.
Expert en développement et déploiement d'applications métier complexes	• Diplôme de niveau minimum bac+5 (Programmeur, informatique, électronique). • Avoir au moins 10 d'expériences dans le développement de logiciel • Expériences dans le développement d'au moins 5 applications d'envergure nationale ;

	• Maîtrise de déploiements d'envergure ou nécessitant une compétence technique particulière. • Être capable de la conduite du déploiement d'application en adéquation aux besoins des utilisateurs. • Connaissance générale des normes et des procédures de sécurité informatique ; • Connaissance générale des standards de développement d'application ; • Connaissance générale des licences de logiciels (notamment pour le choix et l'utilisation de composants logiciels) ; • Connaissance générale des principes éthiques et de la réglementation afférentes à l'utilisation, au traitement et à la conservation des données à caractère personnel ;
Expert sécurité des systèmes d'information,	• Diplôme du niveau minimum Bac +5 spécialisé en sécurité informatique et/ou télécoms, sécurité des systèmes informatiques et des réseaux, sécurité, cryptologie et codage de l'information... ; • Expérience d'au moins 10 ans dans le domaine de la sécurité des systèmes d'information ; • Certifications CISM, CISA, CISSP recommandées ; • Maîtrise des normes et procédures de sécurité et des outils et technologies qui s'y rapportent : firewall, antivirus, cryptographie, serveurs d'authentification, tests d'intrusion, PKI, filtrages d'URL... ; • Maîtrise des réseaux et systèmes ;
Expert en identité numérique	• Au moins un master dans un domaine pertinent. • Au moins 8 ans d'expérience dans la conception et la mise en œuvre de systèmes d'identité numérique, en particulier dans les pays en développement. • Connaissance des normes et technologies mondiales en matière d'identité numérique et des tendances émergentes.
Spécialiste du partage des données et de l'interopérabilité	• Au moins un master dans un domaine pertinent. • Au moins 8 ans d'expérience dans l'élaboration et la mise en œuvre de cadres de partage de données et d'interopérabilité, idéalement dans un contexte gouvernemental. • Connaissance des normes et réglementations en matière de protection des données et de la vie privée.
Expert gestion du changement	• Diplôme supérieur minimum BAC+5 en systèmes d'information, en informatique ou dans un domaine connexe. • Au moins 10 ans d'expérience dans la conception et la mise en œuvre de projets TIC à grande échelle. • Au moins 5 ans d'expérience dans la conduite et l'accompagnement du changement dans une Administration publique ; • Expérience avérée dans la conduite et l'accompagnement du changement dans le cadre d'un ou plusieurs projets ou missions de développement d'ampleur similaire.

Expert métier en politique publique	• Diplôme en sciences politiques, administration publique, relations internationales ou domaine connexe • Minimum de 5 ans d'expérience dans la conception, la mise en œuvre ou l'évaluation de politiques publiques • Expérience avérée dans le conseil pour les organismes gouvernementaux ou des organisations internationales • Connaissance approfondie des processus de formulation et d'implémentation de politiques publiques. • Bonne compréhension des enjeux politiques, sociaux et économiques du Sénégal
Expert Juridique en droit des TICs	• Diplôme supérieur minimum BAC+5 en droit avec une expérience professionnelle d'au moins cinq (05) ans dans la réglementation des TICS et/ou de l'économie numérique (transactions électroniques, protection des données, cybersécurité, identification numérique, etc.) ; • Expérience prouvée des grandes transactions commerciales dans le secteur des TICs (en tant que conseiller, organisateur d'appels d'offres concurrentiels, rédacteur de la documentation juridique, etc.), avec une expérience professionnelle dans les pays en développement en général et en Afrique en particulier. • Réalisation de deux (02) missions similaires dans le secteur des TIC ; • Diplôme de droit et expérience en droit des TIC, en particulier dans les domaines de l'identité numérique, de la protection des données et des transactions électroniques. • Une bonne connaissance du contexte juridique et réglementaire du Sénégal serait un avantage.