

Passation des Marchés de Services de Consultants
N° SN-MCTN-567516-CS-INDV

**Termes de références pour le recrutement d'un Ingénieur
Cybersécurité pour l'opérationnalisation de la Plateforme
d'Interopérabilité Nationale du Sénégal (PINS)**

- **Réf. SN-MCTN-567516-CS-INDV**
- **Projet :** Projet d'Accélération de l'Economie Numérique au Sénégal (PAENS)
- **Pays :** Sénégal
- **Financement :** Banque Mondiale / Crédit : IDA 72690
- **Client :** Gouvernement du Sénégal
- **Autorité Contractante :** Ministère des Télécommunications et du Numérique (MTN),
- **Partenaire de mise en œuvre sur la mission :** SENUM
- **Numéro du Projet :** P172524 SEN/IDA

Août 2026

1 CONTEXTE

Le Projet d'Accélération de l'Économie Numérique au Sénégal (PAENS) a été lancé le 28 juin 2024 par le ministère de la Communication, des Télécommunications et du Numérique, pour un montant de 95 milliards de Francs CFA sur cinq ans (2023 – 2028) de la Banque mondiale.

L'objectif principal de ce programme est d'étendre l'accès à une connectivité large bande abordable et résiliente face aux changements climatiques, tout en améliorant l'adoption numérique des services gouvernementaux en ligne et des dossiers médicaux électroniques. Il suscite un énorme intérêt auprès de l'écosystème numérique et surtout auprès de la population représentée au lancement par plusieurs associations de consommateurs.

Dans le cadre de la mise en œuvre du New Deal Technologique, le Sénégal poursuit le développement de son Infrastructure Publique Numérique (DPI) comme socle de transformation des services publics, d'amélioration de l'expérience usager et de renforcement de la souveraineté numérique. La plateforme interopérabilité, déployée comme un produit structurant de la DPI, entre désormais dans une phase d'opérationnalisation. Cette phase requiert la mise en place d'une organisation adaptée afin d'en assurer l'exploitation durable, la qualité de service, la sécurité et la montée en charge.

À cet effet, SENUM SA, en charge de l'exploitation de la plateforme nationale d'interopérabilité PINS, a défini une organisation cible du RUN PINS combinant des compétences déjà disponibles en interne et des ressources complémentaires à recruter, notamment :

- **Un (1) Manager Business Unit – Interopérabilité ;**
- **Deux (2) Développeurs Full Stack ;**
- **Un (1) Développeur Back-End /Intégrateur ;**
- **Un (1) Ingénieur DevOps ;**
- **Un (1) Architecte Solutions ;**
- **Un (1) Ingénieur Fonctionnel ;**
- **Deux (2) Techniciens Support Systèmes et Réseaux informatiques ;**
- **Un (1) Ingénieur Cybersécurité**

Ces ressources spécialisées seront chargées de soutenir SENUM SA dans l'exploitation opérationnelle, l'évolution et l'appropriation de la plateforme PINS

Les présents termes de référence concernent le recrutement de **l'Ingénieur Cybersécurité dont la fiche détaillée figure en annexe 1.**

2 OBJECTIFS

L'objectif globale de ces recrutements est de renforcer les capacités opérationnelles de SENUM SA afin d'assurer une exploitation efficace, sécurisée et pérenne de l'écosystème PINS,

Plus spécifiquement, les ressources recrutées auront pour mission de :

- Assurer le maintien en conditions opérationnelles et la disponibilité de la plateforme ;
- Soutenir l'intégration progressive des systèmes et acteurs publics ;
- Garantir des niveaux élevés de sécurité, de performance et de qualité de service ;
- Accompagner les administrations utilisatrices dans l'intégration et l'usage de la plateforme ;
- Contribuer à la documentation, aux procédures et au transfert de compétences

3 PORTÉE DES PRESTATIONS

Les ressources globalement recrutées interviendront, sous la supervision de SENUM SA, sur les activités suivantes:

- Exploitation technique et applicative de la plateforme PINS ;
- Support au RUN et à la gestion des incidents ;
- Développement et évolution des interfaces et composants applicatifs ;
- Intégration technique des systèmes métier des administrations ;
- Accompagnement fonctionnel des utilisateurs ;
- Documentation technique et reporting opérationnel.

N.B : Les fiches de postes des profils sont en annexes

4 CALENDRIER

La durée totale de la mission est prévue pour une durée d'un (1) an renouvelable. Un planning opérationnel détaillé sera établi au démarrage.

5 LIVRABLES ATTENDUS

Les principaux livrables incluent :

- Un rapport de prise en charge des activités ;
- Des rapports d'exploitation /d'activité périodiques (mensuels et semestriels) selon un format à définir par la SENUM SA dans les cinq (5) jours qui suivent le mois ;
- Des procédures techniques et fonctionnelles ;
- Des notes d'évolution et de capitalisation ;
- Un rapport final de mission au plus tard un (1) mois après l'achèvement des prestations.
- Un rapport de transfert de compétences
- D'autres livrables complémentaires et nécessaires à la bonne exploitation de la solution seront produits au fil de l'eau et selon les nécessités d'intégration des cas d'usage, notamment :

Profils	Livrables spécifiques
Manager de business Unit	– Feuille de route d'implémentation des use cases et évolution – Document de conception générale (cahier des charges, ...)
Architecte solution	– Document d'architecture technique actualisé
Ingénieur DevOps	– Documentation d'installation des plateformes et des environnements – Manuel d'exploitation et d'administration de la plateforme – Composants techniques déployés sur les environnements de développement, test et production
Développeurs	– Codes sources documentés de la plateforme
Ingénieur fonctionnel	– Processus métier et architecture fonctionnelle
Technicien support	– Rapport de résolution des incidents – Remontée des besoins d'évolution
Ingénieur cybersécurité	– Scan et Pentest – Rapport d'audit de sécurité

6 LIEU DE LA PRESTATION

Les collaborateurs auront à assurer leur fonction aux seins des locaux de Sénégal Numérique Sis Pikine Technopole ou Annexes Almadies.

Ils seront soumis aux horaires appliquées à la SENUM SA

7 LOGISTIQUE

Les consultants assureront leur logistique personnelle nécessaire à la bonne réalisation des prestations.

8 BUREAU

SENUM SA mettra à disposition le matériel et les environnements techniques nécessaires, un cadre de travail adéquat aux prestataires.

ANNEXE : FICHES DE POSTE DE L'INGÉNIEUR CYBERSÉCURITÉ X-ROAD

Intitulé du poste : Ingénieur Cybersécurité X-Road	
Nature du poste : Opérationnel	Contrat : CDD 1 an
Direction d'affectation : Digital & IA Factory	Supérieur hiérarchique : Manager BU Interopérabilité
Descriptif de la fonction : L'Ingénieur Cybersécurité X-Road assure la conception, le déploiement et l'exploitation sécurisée de la plateforme d'interopérabilité basée sur X-Road. - Il garantit la confidentialité, l'intégrité, l'authenticité et la traçabilité des échanges inter-administrations. - Il sécurise les Security Servers, le Central Server et les services de confiance PKI associés. - Il définit les règles de durcissement, de contrôle d'accès, de certificats et de segmentation réseau. - Il assure la supervision des journaux, vulnérabilités et incidents de sécurité de la plateforme. - Il accompagne l'intégration sécurisée des organismes membres, services et API. - Il contribue aux audits, tests, PRA/PCA et à l'amélioration continue de la sécurité.	
Missions	
- Garantir l'architecture de sécurité et l'exploitation sécurisée de la plateforme X-Road et de ses composants critiques. - Administrer la sécurité des Security Servers, du Central Server et des services de confiance associés. - Définir et appliquer les règles de durcissement, de contrôle d'accès, de chiffrement et de segmentation réseau. - Superviser les événements de sécurité, les journaux X-Road et leur intégration au SIEM/SOC. - Piloter la gestion des vulnérabilités, correctifs, audits et plans de remédiation de la plateforme. - Sécuriser l'intégration des membres, sous-systèmes, services et API échangés via X-Road. - Contribuer à la continuité d'activité, au PRA/PCA, à la documentation et à l'amélioration continue de la sécurité.	
Activités	
- Configurer, durcir et maintenir les Security Servers, Central Server et composants d'administration X-Road. - Administrer les certificats d'authentification et de signature, TLS/mTLS et leur cycle de vie. - Assurer l'intégration avec les services PKI : CA, OCSP, horodatage (TSA) et, si applicable, HSM. - Définir les règles de pare-feu, segmentation réseau, flux, ports et accès d'administration nécessaires à X-Road. - Mettre en œuvre les contrôles IAM, MFA, gestion des privilèges, secrets et comptes techniques. - Centraliser et analyser les journaux X-Road ; intégrer les alertes et événements au SIEM/SOC. - Réaliser le suivi des vulnérabilités, CVE, correctifs, configurations de sécurité et plans de remédiation. - Participer à la gestion des incidents, aux investigations, RCA et exercices de réponse aux incidents. - Accompagner l'onboarding des membres et effectuer les revues de sécurité des services/API et flux de données. - Documenter les procédures d'exploitation sécurisée, sauvegarde/restauration, PRA et indicateurs de sécurité.	
Compétences requises pour le poste	

Profil du poste : Diplôme et domaine de formation requis : - Bac +5 en Cybersécurité, Informatique, Systèmes et Réseaux, Télécommunications ou domaine équivalent. - Une certification en sécurité (CISSP, ISO 27001, Security+, CEH ou équivalent) et/ou PKI/Linux serait un atout majeur. Nombre d'années d'expériences professionnelles : - Minimum 5 ans d'expérience en cybersécurité des systèmes, réseaux ou plateformes critiques, incluant durcissement, PKI, supervision et gestion des incidents. - Une expérience sur X-Road ou une plateforme d'interopérabilité, d'échange de données ou de services de confiance est fortement souhaitée.	Compétences exigées : - Bonne maîtrise de l'architecture X-Road : Security Server, Central Server, configuration, membres, sous-systèmes et services. - Maîtrise des principes PKI/X.509, TLS/mTLS, certificats, signatures, OCSP, TSA et gestion des clés. - Très bonne connaissance de Linux et du durcissement des systèmes, services et comptes d'administration. - Solides compétences en sécurité réseau : pare-feu, segmentation, routage, DNS, VPN, reverse proxy et load balancing. - Maîtrise de la journalisation, supervision et corrélation des événements avec des outils SIEM/SOC. - Expérience en gestion des vulnérabilités, CVE, patch management, audits techniques et plans de remédiation. - Connaissance des mécanismes IAM, MFA, RBAC, moindre privilège, secrets et gestion des comptes techniques. - Bonne compréhension des API et services Web (REST/SOAP), de l'authentification et des échanges inter-systèmes. - Compétences en scripting et automatisation : Bash, Python, Ansible ou équivalents. - Capacité à gérer les incidents de sécurité, PRA/PCA, documentation, procédures et exigences de conformité. Qualités requises : - Rigueur, intégrité et sens de la confidentialité. - Capacité d'analyse et de résolution de problèmes. - Esprit d'équipe et aptitude à travailler avec des acteurs multiples. - Autonomie, réactivité et culture d'amélioration continue.	
Liens Fonctionnels	Moyens de travail	Liens Externes/Extérieurs
Dans le cadre de ses missions, il interagit de façon permanente avec la Digital Factory, les équipes systèmes/réseaux, le SOC et les équipes d'intégration.	Les outils de travail sont à la charge du consultant	Organismes membres de X-Road, autorités/services de confiance PKI, partenaires et prestataires techniques.