

REPUBLIQUE DE GUINEE
UNITE DE COORDINATION ET D'EXECUTION DES PROJETS
PROGRAMME D'IDENTIFICATION UNIQUE POUR L'INTEGRATION ET L'INCLUSION SOUS
REGIONALE (WURI) – PRIMATURE
SOLLICITATION DE MANIFESTATIONS D'INTERET
RECRUTEMENT D'UN(E) INGENIEUR(E) EN SECURITE RESEAUX DU PROGRAMME WURI

1. Le Gouvernement de la République de Guinée a reçu un financement de l'Association internationale de développement (IDA) dans le cadre du Programme d'identification unique pour l'intégration et l'inclusion sous régionale (WURI), et a l'intention d'utiliser une partie du montant de ce financement pour effectuer les paiements au titre du contrat suivant : *Recrutement d'un(e) Ingénieur en sécurité réseau du programme WURI*.
2. L'objectif : Le programme WURI vise la mise en place d'un système d'identification unique s'insérant dans le cadre de la CEDEAO en tant que levier de développement socioéconomique. Il consiste à « augmenter le nombre de personnes en Guinée qui ont une preuve d'identité unique reconnue par le Gouvernement facilitant leur accès aux services ». Il est divisé en trois composantes : i) Renforcement du cadre juridique et institutionnel ; ii) Mise en place d'un système d'identification de base fiable et inclusif ; iii) Promotion de l'accès aux services au travers des documents d'identité

Mission du consultant

Placé sous l'autorité du Chef de projet, le Consultant est responsable de l'administration des équipements réseau et sécurité du SID pilote ainsi que de toute l'infrastructure. Il est chargé de :

- Connaître les standards en matière de sécurité et réaliser la veille technologique en matière de solution et infrastructures de sécurité des données ;
 - Développer des normes de sécurité et réaliser le référentiel sécurité ;
 - Participer à l'élaboration, la formalisation et l'application des documents techniques (spécification, document d'architecture, document d'exploitation, etc.) ;
 - Réaliser le design et mettre en place les mesures de sécurité pour la gestion des données et des infrastructures en termes de confidentialité, d'intégrité et de disponibilité ;
 - Gérer la mise en œuvre de l'architecture réseau ;
 - Adapter les bibliothèques cryptographiques logicielles pour les besoins du projet ;
 - Évaluer les solutions de sécurité des données et infrastructures et définir les orientations de l'utilisation des algorithmes cryptographiques dans le système d'identification ;
 - Déployer les services de sécurité (authentification, chiffrement, signature électronique, ..) ;
 - Réaliser des appréciations de risques, la mise en œuvre et le suivi des plans de traitement ;
 - Fournir des rapports techniques et des documents sur les résultats des évaluations ;
 - Garantir une opérationnelle conforme aux enjeux et la sécurité des applications en production et hors production et Effectuer la surveillance et alerte sur parc ;
 - Rédaction et mise à disposition de différents guides (manuel de procédures, guide de prise en main, charte d'utilisation des équipements...) ;
 - Préparer les rapports d'activité et effectuer le reporting au Directeur Technique de l'UGP.
3. L'Unité de Gestion de Coordination du Projet (WURI) invite les candidats (« Consultants individuels ») admissibles à manifester leur intérêt à fournir les services décrits ci-dessus. Les Consultants intéressés doivent fournir les informations démontrant (*documentation en langue française uniquement*) qu'ils possèdent les qualifications requises et une expérience pertinente pour l'exécution des Services.

Qualifications requises :

Le(a) candidat (e) devra:

- Etre titulaire d'un diplôme d'ingénieur en sécurité Informatique, en cryptographie, intégrateur / administrateur système ou équivalent au moins ;
- Avoir une expérience d'au moins dix (10) ans en sécurité des systèmes d'informations justifiée d'une expérience d'au moins cinq (5) ans dans un poste similaire ou dans le développement et la définition d'architecture et de sécurité de systèmes d'information (serveurs, réseau, cryptographie PKI, HSM, solutions d'authentification) ; dans le design des règles et police de sécurité ; dans la configuration des firewalls et des équipements de sécurité ;
- Justifier d'une première expérience significative, au moins 5 ans, en intégration et administration de systèmes et d'infrastructures matérielles, réseaux et Cloud, en déploiement IAC de services Cloud (Azure et/ou AWS), Déploiement de conteneurs Docker, Mise en place et configuration d'outils Open Source ;
- Disposer des certifications NSE Fortinet (Network Security Expert), certification de la sécurité réseau (CEH, ECSA, CISA) ou équivalent seront un plus ;
- Etre bilingue : excellent niveau en Français et Anglais (capacité de rédiger des rapports techniques et documents ainsi que de soutenir des conversations de tout genre).

CONNAISSANCES :

Connaissances approfondies des solutions de sécurité des terminaux :

- Environnement: Windows, Linux/Redhat, administration de la plateforme, création de templates Kubernetes : Connaissances des technologies open source et open standard ;
- Maîtrise des référentiels de bonnes pratiques SI (ITIL, DevOps) ;
- Connaissances des protocoles et sécurité réseaux : TCP/IP; Ethernet; LAN, WAN, WLAN, IPV6, BGP, etc ...;
- Connaissance des Technologies internet SSH, FTP, SFTP, HTTP(s), SNMP ;
- Connaissance approfondie en sécurité réseau: politiques de sécurité, Cryptographie (PKI Interne, Gestion des certificats et clés etc), Authentification forte (RSA SecurID, etc.), Firewall (Fortinet, Cisco ASA), VPN, IPsec/SSL, Proxy/Reverse proxy (Citrix, etc.) ;
- Virtualisation (vSphère/vCenter, Hyperload) Loadbalancing , Clustering et Autoscaling ;
- Connaissance en algorithme et une expérience sur la sécurisation des SID sont des atouts ;
- Connaissance en sécurité des infrastructures cloud ;
- Professionnalisme, méthodique avec un esprit d'analyse et de synthèse ;
- Bonne qualité relationnelle et aptitude du travail en équipe ;
- Avoir une appétence pour les technologies suivantes open source/open standard.

4. LIEU ET DUREE DE LA MISSION

Le Contrat aura une durée initiale d'un (1) an renouvelable sous-réserve de performance. Il sera exécuté dans les locaux de l'UGP à Conakry

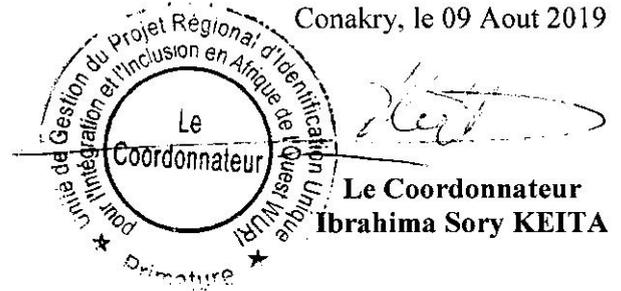
5. Le recrutement se fera suivant la méthode de sélection de consultants individuels conformément aux règlements de passation des marchés pour les Emprunteurs sollicitant le Financement de Projets d'Investissement (FPI).
6. Les Consultants intéressés peuvent obtenir des informations supplémentaires, au sujet des Termes de Reference sur demande à l'adresse ci-dessous et aux heures suivantes du lundi au jeudi de 9h à 16h 00 et le vendredi de 9h à 13h 00, mao.sory@gmail.com / ssekoumamie@gmail.com / fantabiutu@gmail.com .
7. Le dossier de candidature écrite doit être accompagné des pièces suivantes :
 - *Curriculum vitae (CV) signé par le candidat ;*
 - *Lettre de motivation signée par le candidat ;*
 - *Les attestations de travail ou contrat de travail etc. ;*

- *Diplômes attestés ou légalisés* et déposées à l'adresse ci-dessous en personne, par courrier ou par courriels électroniques : mao.sory@gmail.com, ssekounamie@gmail.com, fantabintu@gmail.com au plus tard le **02 Septembre 2019 à 11 heures**.

8. Programme d'identification Unique pour l'Intégration et l'inclusion sous Régionale (WURI), Camayenne, Immeuble résidence Camayenne, 3ème étage – derrière la CENI, Tél. : (+224) 624 21 22 11/622 47 42 18.

Le dossier de candidature doit porter la mention « **Recrutement d'un(e) Ingénieur en sécurité réseau du programme WURI.** »

Conakry, le 09 Aout 2019



The stamp is circular with the text "Unité de Gestion du Projet Régional d'Identification Unique pour l'intégration et l'inclusion en Afrique de l'Ouest WURI" around the perimeter and "Primature" at the bottom. In the center, it says "Le Coordonnateur". A handwritten signature is written over the stamp.

**Le Coordonnateur
Ibrahima Sory KEITA**