Termes de référence (TdR) pour l'acquisition de services informatiques

La Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH,

Coopération allemande au développement en Mauritanie,

cherche une

entreprise locale spécialisée en audit informatique

pour

Audit de la plateforme numérique KHIDMATY

Lieu de travail : Nouakchott

Durée et période de la prestation : 12 semaines entre septembre et décembre 2026

Délai de soumission de l'offre :

Termes de Références

AO :10040956

Subject of the tender procedure:

Transaction number:

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Titre du projet :

Promotion de la transformation numérique (DIGITAL-Y)

Pays :

République Islamique de Mauritanie

Sujet de l'appel d'offres :

Audit technique, de sécurité et de conformité de la plateforme numérique KHIDMATY

Numéro de traitement/ centre de coûts :

G-012396

Numéro de transaction:

0. Liste des abréviations

AN-État : Agence Numérique de l'État

API : Application Programming Interface (Interface de programmation applicative)

GDPR : General Data Protection Regulation (Règlement général sur la protection des données)

GIZ: Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

JE : Jour(s) d'expert·e

JWT : JSON Web Token (Format de jeton pour l'authentification et la transmission sécurisée des informations)

MTNMA : Ministère de la Transformation Numérique et de la Modernisation de l'Administration

PRA : Plan de Reprise d'Activité

RBAC : Role-Based Access Control (Gestion des accès basée sur les rôles)

TLS : Transport Layer Security (Protocole de sécurisation des échanges)

WCAG : Web Content Accessibility Guidelines (Normes d'accessibilité des contenus Web)

PARTIE A - Informations générales

1. Contexte

La Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH aide le gouvernement fédéral allemand à réaliser ses objectifs en matière de coopération internationale pour le développement durable. En Mauritanie, la GIZ met entre outre en œuvre le projet « Promotion de la transformation numérique (DIGITAL-Y) » de la coopération allemande. Le projet accompagne le ministère mauritanien de la transformation numérique et la modernisation de l'administration (MTNMA) dans le développement des solutions numériques nouvelles, cohérentes et centrées sur les citoyens.

Dans le cadre de l'Agenda National de Transformation Numérique, le gouvernement de la République Islamique de Mauritanie a déployé la plateforme « KHIDMATY », composée d'une application mobile (Android et iOS) et d'un portail web accessible à l'adresse https://khidmaty.gov.mr/. Cette solution stratégique, éditée par le MTNMA, dématérialise l'accès aux services publics essentiels : état civil, titres sécurisés, paiement des infractions routières, signalement et dépôt de plaintes.

La plateforme agit comme tiers de confiance numérique et manipule des données critiques : données d'identité (NNI, biométrie), données transactionnelles, documents officiels. Avec plus de 100 000 téléchargements cumulés sur Google Play, KHIDMATY constitue une infrastructure d'État critique.

Face à la montée des cybermenaces, à l'impératif de souveraineté numérique et aux obligations issues de la loi n° 2017-020 relative à la protection des données à caractère personnel, un cabinet d'audit qualifié est cherché afin de réaliser une revue à 360 degrés de la solution KHIDMATY. Le principal bénéficiaire de cette prestation est le MTNMA.

L'objectif général de la mission est d'évaluer et d'attester que l'écosystème KHIDMATY offre un niveau de confidentialité, d'intégrité, de disponibilité et de traçabilité conforme aux meilleures pratiques internationales (OWASP MASVS L2, OWASP ASVS, NIST CSF, et bonnes pratiques inspirées de la norme ISO/IEC 27001) ainsi qu'à la loi mauritanienne n° 2017-020.

Les **objectifs spécifiques** comprennent :

- Valider la posture de sécurité de l'application mobile selon OWASP MASVS niveau L2 et de l'application web selon OWASP ASVS niveau 2 minimum.
- Auditer la performance et la scalabilité face à une charge simulée de 50 000 utilisateurs simultanés.
- Vérifier la conformité réglementaire (loi n° 2017-020, RGPD).
- Évaluer l'expérience utilisateur, en particulier le tunnel d'enrôlement biométrique.
- Produire un plan d'action correctif (PAC) priorisé et chiffré en jours/homme.

2. Exigences auxquelles doit satisfaire la prestation

2.1 Concept général

Description de la plateforme Khidmaty

Lancée en 2024 et développée par MTNIMA en partenariat avec l'Agence Numérique de l'État (AN-ETAT), la plateforme gouvernementale Khidmaty est le guichet numérique unique de la Mauritanie, permettant aux citoyens, aux entreprises et à la diaspora d'accéder en ligne à un nombre croissant de services publics et de démarches administratives, progressivement enrichis grâce à l'intégration de nouvelles applications. Accessible via le web et les stores mobiles, la plateforme repose sur une authentification sécurisée assurée par l'identité numérique nationale Houwiyeti. Les applications gouvernementales et les données des citoyens sont hébergées par l'etat, qui en garantit la sécurité, l'intégrité et la confidentialité, contribuant à la souveraineté numérique du pays. La plateforme vise à résoudre les problèmes de lenteur administrative, de déplacements physiques et d'accès inégal aux services publics, avec pour objectif de simplifier les démarches, d'améliorer l'efficacité de l'administration et de renforcer l'inclusion numérique.

Elle couvre déjà un large éventail de services opérationnels qui illustrent son étendue fonctionnelle : la création d'entreprise en ligne — regroupant en une seule démarche l'immatriculation au Registre de Commerce, l'inscription fiscale et l'affiliation à la CNSS — ainsi que la demande d'agrément au Code des Investissements ; le Système Numérique du Trafic Routier (notification des infractions au code de la route) et l'inscription universitaire en ligne « Tesjil » ; la demande de permis de construire, accessible dans les neuf communes de Nouakchott ; plusieurs services de la SOMELEC et la demande de casier judiciaire dématérialisée. Le portail intègre également l'application de signalement « Ain », et douze nouvelles solutions doivent y être ajoutées progressivement, l'objectif à terme étant d'y centraliser l'ensemble des procédures administratives du pays, dont les plus de 800 démarches recensées sur la plateforme « Ijraati » lancée en février 2026.

Son groupe cible comprend l'ensemble de la population mauritanienne, en particulier les utilisateurs disposant d'un smartphone et d'un accès à Internet, avec des niveaux variés d'alphabétisation numérique et de compétences linguistiques (arabe et français). Ce périmètre s'inscrit dans un contexte national où la marge de progression reste importante : la Mauritanie affichait en 2024 un score de 0,3491 sur 1 à l'indice des Nations Unies pour l'administration en ligne (EGDI). Le rôle central de Khidmaty comme point d'entrée unique de l'administration numérique, conjugué au caractère sensible des données traitées, justifie pleinement le présent audit de sécurité, de performance et de conformité.

Élément	**Référence officielle**
Nom de la plateforme	KHIDMATY
Éditeur / Bénéficiaire	MTNIMA
Portail web	https://khidmaty.gov.mr/
Application Android	Package : mr.got.citoyens.platforme — 100 000+ téléchargements
Application iOS	App Store ID : 6736407388 — Version 0.9.2 — iOS 15.5+
Contact officiel	contact@mtnima.gov.mr | +222 44 45 79 00

Couche	Composants ciblés
Mobile Android	APK signé (mr.got.citoyens.platforme). SAST, DAST, anti-tampering, SSL pinning, stockage local, permissions.
Mobile iOS	IPA signé (App Store ID 6736407388). Keychain, ATS, protection des données, entitlements.
Web (Front)	Portail citoyen, espace personnel, back-office d'administration.
API (Middleware)	API Gateway, services REST/SOAP, OAuth2/OIDC, JWT, rate limiting.
Backend & Data	Bases de données, intégration ANRPTS, intégrations paiement, chiffrement, sauvegardes.
Infrastructure	Hébergement, TLS, WAF, équilibreurs de charge, anti-DDoS, supervision.
Biométrie	SDK de reconnaissance faciale, détection de vivacité, stockage des templates.

L'audit couvrira l'intégralité de la chaîne de valeur numérique de la plateforme KHIDMATY.

Cadre de mise en œuvre chez le partenaire

Le contractant

Le MTNMA, va fournir au contractant suite au lancement du projet (J0) des informations supplémentaires sur le portail Khidmaty, y compris par exemple :

- Schéma d'architecture global, Accès opérationnel à la préproduction avec comptes de test multi-profils, APK Android signé et IPA iOS signé et documentation complète des APIs, cartographie des données personnelles traitées, documentation du mécanisme de chiffrement et de la procédure de suppression des comptes, l'accord de non-divulgation (NDA) et lettre d'autorisation d'audit signés.
- Stack technologique et inventaire des composants, modèle de données, dictionnaire des données sensibles, documentation du SDK biométrique, politique de sécurité du système d'information (PSSI), matrice RBAC, registre des traitements, AIPD si elle existe, liste des sous-traitants, procédures d'exploitation, PCA, PRA, configuration du monitoring, politique de logs, volumétrie réelle, cibles de performance, statistiques d'usage et d'erreurs, organigramme des équipes, liste nominative des points de contact.

La collaboration entre le contractant et le MTNMA s'organise selon les modalités suivantes. Le MTNMA désigne un référent technique et un référent métier, principaux interlocuteurs du contractant pendant toute la durée de la mission et chargés de faciliter l'accès aux informations, aux environnements et aux équipes concernées. La coordination s'organise

autour d'une réunion de cadrage au démarrage (J0), de points d'avancement réguliers et d'une réunion de restitution à l'issue de chaque jalon ou lot de prestations.

Tout accès aux environnements (préproduction et, le cas échéant, production dans un cadre encadré) et aux données n'intervient qu'après signature du NDA et de la lettre d'autorisation d'audit. Les accès accordés sont nominatifs, tracés, limités au strict nécessaire et révoqués à la fin de la mission, avec remise d'une attestation de destruction des données. Le contractant s'engage à préserver la confidentialité, l'intégrité et la disponibilité de la plateforme, à coordonner avec le MTNMA toute action susceptible d'affecter le service (notamment lors des tests d'intrusion) et à signaler sans délai toute vulnérabilité critique découverte.

De son côté, le MTNMA s'engage à mettre à disposition, dans les délais convenus, la documentation et les accès prévus au lancement, ainsi que la disponibilité des équipes techniques et métier nécessaires aux entretiens et à la validation des constats. Les livrables sont soumis au MTNMA et à la GIZ pour revue et validation, le contractant intégrant les retours avant la version finale.

Formation et transfert de compétences sur les bonnes pratiques

Au-delà de la remise des livrables, la mission comprend un volet de transfert de compétences visant à renforcer l'autonomie des équipes du MTNMA et de l'AN-ETAT dans la durée. À l'issue de l'audit, le contractant anime une session de restitution et de formation aux bonnes pratiques portant notamment sur les recommandations priorisées et leur plan de remédiation, les bonnes pratiques de développement et de configuration sécurisés (référentiels OWASP ASVS/MASVS, durcissement des serveurs et des composants), la gestion des vulnérabilités et des correctifs, la protection des données personnelles et la conformité (loi n° 2017-020, RGPD), ainsi que la surveillance, la journalisation et la réponse aux incidents. Cette session s'appuie sur des cas concrets issus de l'audit et donne lieu à la remise d'un support de formation réutilisable (présentation, guide des bonnes pratiques et check-lists). Ses modalités — format (présentiel ou distanciel), durée, nombre de participants et profils visés (équipes techniques, sécurité et métier) — sont précisées au kick-off (J0) en concertation avec le MTNMA. Le cas échéant, une formation dédiée complémentaire, par exemple une sensibilisation à la sécurité pour un public élargi ou la prise en main d'outils spécifiques, pourra être définie et intégrée aux lots de prestations.

2.2 Exigences en matière d'infrastructure

L'hébergement du portail Khidmaty est assuré au sein de l'infrastructure de l'état mauritanien, qui garantit la sécurité, l'intégrité et la confidentialité des données et des applications gouvernementales. La plateforme n'est pas un système isolé : elle s'interconnecte avec d'autres systèmes gouvernementaux (identité numérique Houwiyeti, registres des administrations partenaires, moyens de paiement nationaux), et ses dispositifs de sécurité périmétrique (pare-feu, passerelles, segmentation réseau) peuvent être mutualisés avec d'autres composants de l'infrastructure de l'État. Le projet décrit dans ces TDR est limité strictement au périmètre de Khidmaty : aucun test ne sera mené sur les systèmes tiers ou l'infrastructure partagée sans autorisation écrite préalable, et toute action susceptible d'affecter la disponibilité (notamment les tests d'intrusion) sera planifiée et coordonnée avec le MTNMA.

Exigences en matière de sécurité

Au-delà de l'identification des vulnérabilités, le contractant est attendu sur la formulation de recommandations concrètes et priorisées visant à renforcer la sécurité de la plateforme

Khidmaty et de son environnement d'hébergement, portant notamment sur la sécurité périmétrique et réseau (pare-feu, passerelles, segmentation et filtrage des flux), la protection des postes et serveurs (antivirus/EDR, durcissement, gestion des correctifs), le chiffrement des données en transit et au repos ainsi que la gestion des clés et des secrets, les mécanismes d'authentification et de gestion des accès (authentification forte/MFA, politique de mots de passe, matrice RBAC, gestion des sessions) et la journalisation, la supervision et la détection des incidents. Chaque recommandation sera hiérarchisée selon sa criticité et sa faisabilité, s'appuiera sur les référentiels reconnus (OWASP ASVS/MASVS, OWASP API Security Top 10, ISO/IEC 27001) et sera assortie d'un plan de remédiation exploitable par les équipes du MTNMA.

2.3 Exigences fonctionnelles et non-fonctionelles et autres exigences

- Sans objet -

3. Taches de la partie contractante

La partie contractante exécute les prestations et lots de prestations suivants (ainsi que les jalons correspondants). Les lots de prestations ne définissent pas un ordre chronologique fixe et peuvent, selon la méthodologie de développement adoptée, être mis en œuvre de manière intégrée.

3.1 Lot de prestation 1 : Lancement

Au démarrage du projet, dans une réunion en présence à Nouakchott, la partie contractante, le bénéficiaire et la GIZ se met d'accord sur la rythme de collaboration, la plateforme technique utilisée pour le travail en commun, les détails concernant les responsabilités respectives, ainsi que la planification du calendrier du projet. Cette première réunion vise également à préciser les aspects de fond liés à la problématique à résoudre, à la définition des objectifs, aux exigences, et aux informations contextuelles pertinentes.

Prestations à fournir par la partie contractante :

- Documentation des accords convenus
- Mise en place d'un environnement de travail (en ligne) adapté

3.2 Lot de prestation 2 : Concept de mise en œuvre

Le concept de mise en œuvre est élaboré par la partie contractante et validé par la GIZ et le bénéficiaire. Il comprend notamment :

- la méthodologie de développement, le calendrier et le plan de publication
- révision et la priorisation des exigences fonctionnelles,
- (pré-)architecture du système, et
- selon la méthodologie choisie : description des cas d'usage et des spécifications système, ou backlog comprenant, par exemple, des histoires utilisateur,

- représentations graphiques et schémas (p. ex. maquettes, parcours utilisateur, schémas de processus, diagrammes entité-relation (ERD) et cas d'usage).

Résultats de travail à fournir par la partie contractante :

Concept de mise en œuvre

3.3 Lot de prestation 3 : Mise en œuvre technique

Module 1 — Audit de sécurité (cyber)

- Tests d'intrusion Black Box, Grey Box et Mobile Specific (Android et iOS).
- Revue de code sécurisé automatisée et manuelle ciblée.
- Audit du SDK biométrique et du flux d'enrôlement.

Module 2 — Architecture et performance

- Stress testing jusqu'à 50 000 utilisateurs simultanés (JMeter, Gatling, k6).
- Revue d'architecture, résilience, haute disponibilité, PCA et PRA.

Module 3 — Fonctionnel et UX/UI

- Analyse heuristique des parcours critiques.
- Matrice de compatibilité sur terminaux d'entrée de gamme et faible connectivité.

Le développement de la solution informatique s'effectue sur la base du concept de mise en œuvre. La méthodologie de développement et le plan de publication déterminent les étapes (itératives) de mise à disposition des fonctionnalités. La partie contractante doit proposer la méthodologie de développement et le concept de déploiement dans le document de conception fonctionnelle (voir le chapitre **Erreur ! Source du renvoi introuvable.**).

Résultats de travail à fournir par la partie contractante :

Code objet ou application opérationnelle et exécutable

- documentation du processus de développement (p. ex. progression, modifications) ;
- code source commenté.

3.4 Lot de prestation 4 : Test et assurance qualité

La partie contractante met en place un environnement de test et réalise, pendant et après le développement, les tests recommandés (p. ex. tests unitaires, d'intégration, de charge). Des tests réguliers doivent également être effectués avec les futur·e·s utilisateur·rice·s de la solution informatique.

Résultats de travail à fournir par la partie contractante :

Concept de test et documentation des tests

- Documentation du retour d'expérience des utilisateur·rice·s ainsi que des corrections effectuées (erreurs, vulnérabilités, failles, etc.)

3.5 Lot de prestation 5 : documentation

Une documentation complète doit être mise à la disposition de la GIZ en temps utile et de manière appropriée. La partie contractante est tenue de donner à tout moment accès à la version actuelle de la documentation. Tous les livrables seront rédigés en français et fournis en deux (2) exemplaires physiques reliés ainsi qu'en un (1) exemplaire numérique sur clé USB chiffrée.

N°	Livrable	Contenu attendu	Responsable
L1	Rapport de cadrage	Planning, méthodologie, PAQ, vérification des prérequis	**Expert 1**
L2	Rapport d'audit de sécurité	Synthèse + technique, CVSS, PoC	**Expert 1**
L3	Rapport d'audit performance & conformité	Charge, points de rupture, cartographie DCP, registre des traitements	**Expert 2**
L4	Rapport UX, fonctionnel & biométrie	Heuristique, biométrie, compatibilité, recommandations	**Expert 3**
L5	Plan d'action correctif (PAC)	Tableau priorisé, chiffrage jours/homme par correctif	**Expert 1 (consolidation)**

3.6 Lot de prestation 5 : Formation

La partie contractante organise une formation technique destinée au personnel informatique du bénéficiaire, d'une durée de 3 jours, pour environ 15 participant·e·s, en langue arabe au MTNMA, afin de renforcer les connaissances et capacités nécessaires à une exploitation durable du système. Les contenus de la formation doivent également être formalisés par écrit.

Résultats de travail à fournir par la partie contractante :

Supports de formation

4. Calendrier et étapes

La durée prévisionnelle du contrat est de 6 mois entre septembre 2026 et février 2027. Les échéances et délais pour l'atteinte des jalons par le contractant sont fixés comme suit :

Jalons	Délais
Réunion de lancement en présence au MTNMA	1 semaine après le début du contrat
Remise du rapport de cadrage (L1)	1 semaine après la réunion de lancement
Comité de pilotage à mi-parcours	6 semaines après le début du contrat
Remise des rapports d'audit — sécurité (L2), performance et conformité (L3), UX et fonctionnel (L4)	9 semaines après le début du contrat

Restitution finale et remise du plan d'action correctif consolidé (L5)	11 semaines après le début du contrat
Formations ont eu lieu (L6)	12 semaines après le début du contrat

5. Octroi de droits d'utilisation (par exemple à des partenaires)

Le prestataire signera un Accord de Non-Divulgation (NDA) strict avant tout accès à la documentation ou aux systèmes. Toutes les données, rapports, scripts de test et vulnérabilités découvertes restent la propriété exclusive et confidentielle de l'État Mauritanien.

À l'issue de la mission, le prestataire fournira une attestation de destruction de l'ensemble des données techniques collectées sur ses propres infrastructures, à l'exception des éléments strictement nécessaires à la traçabilité de la mission.

Toute divulgation publique, totale ou partielle, des informations couvertes par le NDA exposera le prestataire à des poursuites judiciaires, conformément à la législation mauritanienne en vigueur.

6. Protection des données et sécurité de l'information

Les dispositions relatives à la protection des données et à la sécurité de l'information de la version actuelle des conditions générales de contrat de la GIZ (section 1.1. Confidentialité et 1.10 Protection des données) s'appliquent.

Protection des données

L'exécution du contrat peut être associée au traitement de données à caractère personnel par le contractant, telles que (mais sans s'y limiter) des noms et des informations de contact, qui définira seul la nature de ces données et la manière dont ce traitement sera effectué. Dans ce cas, le contractant agira en tant que CONTRÔLEUR DE DONNÉES indépendant et devra respecter seul TOUTES les obligations applicables en matière de protection des données, y compris celles qui découlent des lois régionales et locales. Le contractant ne traite les données à caractère personnel que lorsqu'un objectif donné ne peut être raisonnablement atteint sans ces données. Les principes de protection des données tels que la légalité, la minimisation des données, l'exactitude, la limitation de la finalité, la limitation du stockage, la transparence, l'intégrité et la confidentialité, et la responsabilité, ainsi que les nombreux droits de la personne concernée doivent être dûment pris en compte. La GIZ n'est en aucun cas responsable de ce traitement.

Lorsque le contractant exécute les instructions d'un partenaire de la GIZ concernant un tel traitement, le partenaire est le responsable du traitement des données, et le traitement des données est effectué conformément aux instructions du partenaire ainsi qu'aux lois et normes auxquelles il est soumis.

Si le contractant n'est pas soumis au GDPR et que les lois applicables ne contiennent aucune explication sur les principes et droits de protection des données mentionnés ici, les définitions et significations fournies par le GDPR (Règlement (UE) 2016/679) doivent être prises en compte.

La collecte de données pour le S&E de la GIZ doit être effectuée de manière strictement anonyme, ce qui signifie que toute information relative à une personne physique identifiée ou identifiable ("personne concernée") doit être exclue.

Sauf demande explicite de la GIZ, les évaluations, les rapports, les enquêtes ou toute autre donnée et information partagée avec la GIZ doivent être fournis de manière strictement anonyme, ce qui signifie que toute information relative à une personne physique identifiée ou identifiable ("personne concernée") doit être exclue. En particulier, les données relatives, par exemple, au sexe, à l'âge, à la santé, à la religion ou à l'appartenance ethnique doivent être fournies de manière agrégée.Les services du contractant doivent être fournis en français avec l'exception de l'application, qui doit être développée en français et en arabe.

7. Sécurité de l'information

- Sans objet -

8. Langue

La partie contractante exécute les prestations en langue arabe ou français. Tous les livrables seront rédigés en français.

PARTIE B – Exigences pour l'offre

9. Concept technico-méthodologique

Lors de l'élaboration conceptuelle de son offre (approche technique et méthodologique, gestion de projet, et le cas échéant autres exigences), le soumissionnaire doit prendre en compte des objectifs et exigences spécifiques, qui sont précisés ci-après.

9.1 Exigences relatives à la conception technique et méthodologique (point 1 du schéma d'évaluation)

Le soumissionnaire doit expliquer dans son offre comment il prévoit de réaliser les prestations décrites au chapitre 3, le cas échéant en tenant compte d'autres exigences méthodologiques spécifiques indiquées au chapitre **Erreur ! Source du renvoi introuvable.** (conception technique et méthodologique)

Évaluation des exigences

Le soumissionnaire doit évaluer les objectifs et les exigences de la solution informatique (voir chapitres 0 et **Erreur ! Source du renvoi introuvable.**) en termes de faisabilité et indiquer les difficultés particulières, techniques ou non techniques, que la solution à développer devra prendre en considération pour atteindre les objectifs fixés (point 1.1 du schéma d'évaluation).

Gestion de projet et méthodologie de développement

Le soumissionnaire doit décrire son approche en matière de gestion de projet ainsi que sa méthodologie de développement et de mise en œuvre, en tenant compte des lots de prestation décrits (chapitre 3) et du respect des jalons (chapitre **Erreur ! Source du renvoi introuvable.**) (point 1.2 du schéma d'évaluation).

Plan d'opérations / planning d'affectation du personnel

Le soumissionnaire doit présenter et expliciter un plan d'opérations, comprenant également un planning d'affectation du personnel spécialisé qu'il prévoit de mettre en place. Le plan d'opérations doit indiquer les durées d'intervention (périodes et nombre de jours d'expert·e) et en particulier décrire les étapes de travail nécessaires, et intégrer ou compléter les jalons mentionnés au chapitre **Erreur ! Source du renvoi introuvable.** (point 1.3 du schéma d'évaluation).

Concept de test et de documentation

Le soumissionnaire doit décrire sa méthodologie de test et de documentation de la solution informatique, ainsi que les normes et standards de sécurité informatique et de documentation qu'il entend appliquer (point 1.4 du schéma d'évaluation).

9.2 Exigences supplémentaires (section 2 de la grille d'évaluation)

Sans objet

10. Personnel

Le soumissionnaire doit proposer des personnels pour les postes (« expert·e·s ») mentionnés dans ce chapitre et décrits en termes de tâches et de qualifications, sur la base de curriculum vitæ correspondants. **Les exigences relatives au format et au contenu des CV sont décrites au chapitre** Erreur ! Source du renvoi introuvable..

Les qualifications indiquées ci-après correspondent aux exigences permettant d'atteindre le nombre maximal de points dans le cadre de l'évaluation technique.

Par « un an d'expérience professionnelle », il faut comprendre un total cumulé de 12 mois d'expert·e à raison d'au moins 18 jours d'expert·e par mois, sauf si une définition différente est donnée pour certaines qualifications.

10.1 Expert·e 1 : direction de l'équipe *(point 3.1 du schéma d'évaluation)*

Ce poste est celui d'un.e expert.e clé. Pour cet·te expert·e, une déclaration de disponibilité devra être jointe à l'offre.

Tâches de l'expert·e 1 : direction de l'équipe

- Pilotage global de la mission et interface unique avec le MTNIMA
- Animation du comité de pilotage et des points hebdomadaires
- Rédaction et validation du Plan d'Assurance Qualité (PAQ)
- Tests d'intrusion Black Box (attaquant externe non authentifié)
- Tests d'intrusion Grey Box avec comptes citoyen, agent, administrateur
- Tentatives d'escalade horizontale et verticale des privilèges
- Audit mobile Android : analyse APK, contournement root detection, SSL pinning, stockage local (SharedPreferences, Keystore)
- Audit mobile iOS : analyse IPA, Keychain, ATS, entitlements, jailbreak detection
- Audit des APIs REST/SOAP : OWASP API Top 10, JWT, OAuth2/OIDC
- Revue de code sécurisé automatisée (SAST) et ciblée (manuelle) sur fonctions critiques

- Rédaction des PoC (preuves de concept) et scoring CVSS v3.1 de chaque vulnérabilité
- Synthèse managériale et présentation des résultats aux décideurs
- Signature finale du rapport d'audit de sécurité et consolidation du PAC
- Gestion des escalades et des incidents pendant les tests
- Responsabilité globale des livrables
- Responsabilité rédactionnelle des livrables L1 (Rapport de cadrage), L2 (Rapport d'audit de sécurité (synthèse + technique)) et L5 (Plan d'action correctif (PAC)) consolidé.

Qualifications de l'expert·e 1 : direction de l'équipe

Formation (point 3.1.1 du schéma d'évaluation)	Diplôme universitaire (Bac+5) (Master ou diplôme d'ingénieur) en Cybersécurité, Sécurité des Systèmes d'Information, Informatique ou Ingénierie des Systèmes d'Information, complété par des certificats professionnels suivants : - ISO/IEC 27001 Lead Auditor ; - OSCP /OSWE ou CREST CRT/CCT ; - CISSP ou CISM
Langue(s) (point 3.1.2 du schéma d'évaluation)	Connaissances du français au niveau C1 et selon le Cadre européen commun de référence pour les langues
Expérience professionnelle générale (point 3.1.3 du schéma d'évaluation)	12 ans d'expérience professionnelle en cybersécurité, sécurité de l'information ou génie informatique, axés sur les réseaux, la cryptographie et le développement de logiciels sécurisés, acquise au cours des dernières 7 ans.
Expérience professionnelle spécifique (point 3.1.4 du schéma d'évaluation)	Au moins 7 ans d'expérience professionnelle en audit de sécurité et tests d'intrusion offensifs, dont au moins 3 missions portant sur des projets numériques critiques ou gouvernementaux au cours des 5 dernières années, avec une maîtrise démontrée — attestée par au moins une mission d'application concrète — des référentiels OWASP MASVS L2, OWASP ASVS et OWASP API Security Top 10.
Expérience de direction / de management (point 3.1.5 du schéma d'évaluation)	3 ans d'expérience de direction dans des projets numériques ou des équipes multidisciplinaire.
Expérience de la coopération au développement (point 3.1.6 du schéma d'évaluation)	sans objet
Divers (point 3.1.7 du schéma d'évaluation)	Sans objet

10.2 Expert 2 : en architecture, performance et conformité (point 3.2 du schéma d'évaluation)

Tâches de l'expert·e 2

- Revue de l'architecture logique, physique et réseau de la plateforme
- Évaluation de la résilience et de la haute disponibilité (HA)
- Stress tests avec montée en charge progressive jusqu'à 50 000 utilisateurs simultanés
- Identification du point de rupture (breaking point) et des goulets d'étranglement
- Mesure des temps de réponse et de la consommation des ressources
- Revue du Plan de Continuité d'Activité (PCA) et du Plan de Reprise d'Activité (PRA)
- Évaluation des cibles RTO/RPO et de leur faisabilité technique
- Cartographie des données personnelles (catégories, finalités, durées, destinataires)
- Vérification du registre des traitements au sens de la loi n° 2017-020
- Audit de la politique de confidentialité et de sa cohérence multi-canal
- Évaluation des mécanismes de consentement et de la gestion des droits des personnes
- Audit du processus de suppression des comptes et d'effacement des données
- Évaluation de la base légale du traitement des données biométriques
- Production ou revue de l'AIPD (Analyse d'Impact relative à la Protection des Données)

Qualifications de l'expert·e 2

Formation (point 3.2.1 du schéma d'évaluation) :	Diplôme universitaire (master ou diplôme d'ingénierie) en Informatique ou Ingénierie des Systèmes d'Information complétée par des certifications suivants : - TOGAF ou équivalent - Certification cloud (par ex. AWS Solutions Architect Professional, Azure SA Expert ou GCP PCA) - Certification CIPP/E (IAPP) ou DPO certifié AFNOR / Bureau Veritas
Langue(s) (point 3.2.2 du schéma d'évaluation) :	Connaissances de français B2 selon le Cadre européen commun de référence pour les langues
Expérience professionnelle générale (point 3.2.3 du schéma d'évaluation) :	7 ans d'expérience professionnelle en Informatique ou technologie d'information
Expérience professionnelle spécifique (point 3.2.4 du schéma d'évaluation) :	5 ans d'expérience professionnelle spécifique en architecture des systèmes d'information distribués à forte charge (min.100 000 utilisateurs) et sur AIPD/DPIA de services publics Connaissance d'application avérée de la loi mauritanienne n° 2017-020 et du RGPD

	Maîtrise demontré des outils de stress test : JMeter, Gatling, k6, Locust
Expérience de direction / de management (point 3.2.5 du schéma d'évaluation) :	sans objet
Expérience de la coopération au développement (point 3.2.6 du schéma d'évaluation) :	sans objet
Divers (point 3.2.7 du schéma d'évaluation) :	sans objet

10.3 Expert.e 3 en UX, fonctionnel & biométrie

Tâches de l'expert·e

- Analyse heuristique des parcours critiques de l'application
- Évaluation approfondie du tunnel d'enrôlement biométrique (priorité absolue)
- Analyse fonctionnelle du SDK biométrique : taux d'erreur, détection de vivacité, gestion des échecs
- Tests sur terminaux Android d'entrée de gamme répandus en Mauritanie
- Tests sur iPhone supportant iOS 15.5 et versions ultérieures
- Évaluation du comportement en faible connectivité (Edge, 3G, perte de signal)
- Investigation des problèmes utilisateurs documentés sur les magasins d'applications
- Analyse du workflow de paiement et de réconciliation
- Évaluation de l'accessibilité (WCAG 2.1 niveau AA)
- Évaluation de l'internationalisation (français / arabe) et de la qualité linguistique
- Recommandations d'interface priorisées
- Responsabilité technique pour les livrables L4 (Rapport UX, fonctionnel et biométrie et la matrice de compatibilité des terminaux) et contribution au L5 (Plan d'action correctif (volet UX et fonctionnel)).

Qualifications requises pour l'expert·e 3

Formation (point 3.3.1 du schéma d'évaluation)	Diplôme universitaire (master ou diplôme d'ingénierie) en informatique et design graphique (UX/UI) avec une certification NN/g UX Master, HFI CUA ou équivalent
Langue(s) (point 3.3.2 du schéma d'évaluation)	Connaissances du français C1 selon le Cadre européen commun de référence pour les langues

Expérience professionnelle générale (point 3.3.3 du schéma d'évaluation)	7 ans d'expérience professionnelles en UX/UI design, recherche utilisateur et audit fonctionnel
Expérience professionnelle spécifique (point 3.3.4 du schéma d'évaluation)	5 ans d'expérience professionnel spécifique en SDK biométriques (reconnaissance faciale, détection de vivacité), les applications eGov à grande échelle et des méthodes d'analyse heuristique (Nielsen, Bastien-Scapin), de préférence dans les marchés ouest-africains (terminaux low-end, faible connectivité)
Expérience de direction / de management (point 3.3.5 du schéma d'évaluation)	Sans objet
Expérience de la coopération au développement (point 3.3.6 du schéma d'évaluation)	Sans objet
Divers (point 3.3.7 du schéma d'évaluation) :	Sans objet

Toute substitution des experts 2 et 3 en cours de mission doit être validée par écrit par le MTNIMA, le profil de remplacement devant présenter un niveau équivalent ou supérieur.

Le soumissionnaire doit affecter les expert·e·s qu'il propose aux différentes tâches en fonction de leurs qualifications et présenter ces informations de façon claire dans une synthèse placée avant les curriculum vitæ. Il ne faut mentionner dans cette synthèse que des qualifications qui figurent également dans les curriculum vitæ. L'expérience professionnelle doit être attestée par la présence de références pertinentes dans les curriculum vitæ. Il est conseillé de faire une référence explicite aux différentes expériences professionnelles.

Compétences relationnelles des membres de l'équipe
En plus de leurs qualifications techniques, tou·te·s les membres de l'équipe doivent également posséder les qualités suivantes :

- Capacité à travailler en équipe
- Esprit d'initiative
- Aptitude à communiquer
- Compétences socioculturelles et interculturelles
- Démarche orientée vers les partenaires et les clients et efficacité dans l'action
- Esprit interdisciplinaire

Les compétences relationnelles ne sont pas évaluées.

11. Consignes de calcul

Affectation des experts

Dans votre offre, veuillez respecter scrupuleusement le cadre estimatif détaillé prescrit dans les présents TdR (nombre d'expert·e·s et de jours d'expert·e (JE), budgets indiqués dans le bordereau de prix), car ces éléments sont partie intégrante de l'appel d'offres et sont

nécessaires à l'évaluation d'offres comparables sur la base de critères objectifs. Nous tenons à signaler que seules seront rémunérées les prestations qui ont été commandées par la GIZ et exécutées par la partie contractante, et qu'il ne sera pas nécessairement fait appel au nombre total de jours d'expert·e proposés.

Le nombre de jours d'expert·e correspond à des jours de travail entiers.

Expert·e	**Jours d'expert·e**
Expert·e 1 : **Chef de mission / Lead auditeur sécurité & pentest**	40
Expert·e 2 : **Expert architecture, performance & conformité**	28
Expert·e 3 : **Expert UX, fonctionnel & biométrie**	18

Frais de voyage, de matériel, équipements et hébergement

– sans objet –

Ateliers et formations

L'organisation logistique des formations est sous la responsabilité du MTNIMA.

Poste de rémunération flexible

Budget au titre de la rémunération flexible : 3.000 euros

Le budget indiqué ci-dessus est prévu au titre de la rémunération flexible. Ce budget mentionné dans le bordereau de prix est fixe et ne peut pas être modifié. La rémunération flexible vise à permettre un pilotage souple du marché par le·la responsable du marché de la GIZ. L'utilisation par la partie contractante s'effectue conformément au point 21.5 des Conditions contractuelles particulières de la GIZ.

Exigences en co-financements

– sans objet–

PARTIE C – Consignes relatives à la soumission

12. Exigences relatives au format de l'offre

La structure de l'offre doit correspondre à la structure du cahier des charges. Elle doit être lisible (taille de police 11 ou plus) et clairement formulée. La langue dans laquelle l'offre doit être rédigée est le français.

Le concept technico-méthodologique de l'appel d'offres (section 7 du cahier des charges) ne doit pas dépasser 10 pages (non compris la page de couverture, la liste des abréviations, la table des matières et une brève introduction).

Les CV du personnel proposé conformément à la section 9 des TdR doivent être présentés dans le format de l'UE et ne pas dépasser quatre pages. Les CV doivent clairement indiquer le poste occupé par la personne proposée, les tâches qu'elle a accomplies et le nombre de jours d'expertise qu'elle a effectués au cours de la période concernée dans les références spécifiées. Les CV peuvent également être soumis dans une autre langue, à savoir l'anglais.

Nous vous demandons instamment de ne pas dépasser le nombre de pages indiqué.

13. Procédure de sélection

Les soumissionnaires sont invités à soumettre une offre technique et une offre financière conformes au cahier des charges et comme décrit ci-dessous. Les offres incomplètes ou ne respectant les instructions seront exclues. Le marché sera attribué au soumissionnaire ayant obtenu la note la plus élevée après combinaison des notes techniques (70%) et financières (30%). Les offres seront ouvertes à huis clos par la GIZ le plus tôt possible après la clôture des réceptions de dossiers.

14. Consignes relatives à l'envoie des offres

Les candidats intéressés par le présent appel d'offres pourront acquérir le dossier d'appel d'offres (TDRS, Schéma d'évaluation technique, Schéma d'évaluation de l'aptitude, conditions générales et annexes) sans frais au près du bureau de la GIZ Mauritanie, Ilot V 22, **Tel : 00 222 45 25 67 25** au plus tard le **31.08.2026 à 16h 00**.

Jusqu'au 01.09.2026, toutes questions de clarification doivent être formulées en français à l'adresse électronique suivante Email : **MR_Quotation@giz.de** . L'objet du courriel doit être intitulé comme suit : **DAO – 10040956 Audit technique, de sécurité et de conformité de la plateforme numérique KHIDMATY.**

Les offres rédigées en français doivent être facile à lire (ARIAL, taille de police 11) et clairement formulées. Elles doivent être envoyées en format PDF à l'adresse électronique suivante : MR_Quotation@giz.de **au plus tard le 02.09.2026 à 23h59. Les dossiers envoyés hors délais ne seront pas recevables.**

Les contenus externes (tels que les liens conduisant à des pages web) ne seront pas pris en compte

Les offres doivent être envoyées **en 2 courriels séparés** à l'adresse MR_Quotation@giz.de au plus tard à la date limite fixée dans l'avis d'appel d'offres avec pour objet mentionnant le numéro de l'appel d'offre :10040956 suivi par la mention respective « offre technique et dossier administratif » ou « offre financière » et contenir les documents mentionnés ci-dessous.

15. Pièces constitutives de l'offre technique

L'offre technique à envoyer dans un courriel avec objet « 10040956 offre technique et dossier administratif » à l'adresse MR_Quotation@giz.de est composée de :

I. 1 document format PDF pour le dossier administratif :

Portant le nom du cabinet et la mention « Dossier administratif », le fichier doit contenir (dans l'ordre) les documents suivants :

- Dernier rapport annuel administratif (chiffre d'affaires annuels pour 2023, 2024, 2025 ; cf. schéma de l'aptitude) au moins 800.000 MRU par an ; **tamponné et signé, légalisé par un bureau d'audit. Le chiffre d'affaires doit être clairement mentionné et visible.**
- Min. 3 projets de références dans le domaine de développement des services numériques gouvernementaux (dans les trois dernières années) qui prouvent un volume minimum de 700.000 MRU (cf. grille d'aptitude)
- Attestation de non-redevance des impôts (récente, moins de 3 mois) ;
- Attestation de régularité fiscale (récente, moins de 3 mois)
- Numéro d'identification du prestataire (NIF) ;
- Code de conduite paraphé et tamponné ;
- Auto-déclaration droits de l'homme ;
- Relevé d'identité bancaire (RIB)
- Auto-déclaration d'éligibilité

1 document en format PDF pour le dossier technique correspondant aux exigences du chapitres 9-10-11 de la partie B.

16. Pièces constitutives de l'offre financier

L'offre financier à envoyer dans un autre courriel avec pour objet « **10040956 offre financière** » à l'adresse **MR_Quotation@giz.de**

L'offre financière doit inclure tous les frais nécessaires à l'accomplissement de la mission (voir annexe Bordereau des prix) ;

Tous les prix sont exprimés en MRU, hors TVA.

Les prix offerts à la soumission, tels acceptés par la GIZ et ayant fait objet d'un contrat par la suite entre la GIZ et une entreprise, sont fermes et non révisables.

L'absence de l'une des pièces ci-dessus peut entraîner la disqualification de l'offre.

17. L’envoi de l’offre technique et financière dans un seul et même mail entraîne la disqualification de l’offre.

18. **Le délai de soumission de l’offre expire le 02.08.2026**