Envoyé en préfecture le 05/04/2022
Reçu en préfecture le 05/04/2022
Affiché le
ID : 069-256910183-20211210-2022MTNO02-CC

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

C.C.T.P

MAINTIEN EN CONDITION OPERATIONNELLE D'UNE PLATEFORME LOGICIELLE DE GESTION DES IDENTITES ET DES ACCES – SOLUTION LIBRE LEMONLDAP::NG ET PRESTATIONS ASSOCIEES

OBJET DU MARCHE : MAINTIEN EN CONDITION OPERATIONNELLE D'UNE PLATEFORME LOGICIELLE DE GESTION DES IDENTITES ET DES ACCES – SOLUTION LIBRE LEMONLDAP::NG ET PRESTATIONS ASSOCIEES

ARTICLE I. SOMMAIRE

ARTICLE II. PRESTATIONS OBJET DU MARCHE

Le SITIV a déployé en 2018 pour le compte de ses communes adhérentes Corbas, Givors, Grigny, Pierre-Bénite, Rive de Gier, Saint-Chamond, Vaulx, Vénissieux, Sitiv, une plateforme de gestion des identités basées sur les solutions LEMONLDAP::NG, OpenLDAP, LSC et LTB Self Service Password.
Ces solutions sont en licence libre et 100% Opensource.

La plateforme permet aux utilisateurs des collectivités de :
- d'accéder en authentification unique aux application web via des protocoles standard comme CAS, SAMLV2 et OpenIDConnect,
- de bénéficier d'une authentification forte
- d'accéder à un portail applicatif
- de disposer de différentes fonctions complémentaires de gestion de la sécurité liée à l'identité.

Cet outil libre a été identifié comme un des composants de base du nouveau bureau virtuel collaboratif libre de l'agent et de l'élu, construit par le SITIV avec le soutien financier de l'Agence Nationale de Cohésion Territoriale (ANCT) dans le cadre du plan France Relance.

L'objectif de la subvention étant de faciliter le développement d'usages publics et communs d'intérêt général, les productions liées au contrat seront réalisées, documentées et publiées sous licence ouverte incluant leurs sources.

Les licences ouvertes applicables seront arrêtées d'un commun accord entre les Parties.

D'ores et déjà, il est acté que l'ANCT souhaite mettre en œuvre des licences ouvertes « permissives » : la version N du produit ou service soutenu est ouverte, la version ultérieure N+1 peut faire l'objet d'un développement privé ;

Si nécessaire, les Parties pourront s'entendre sur une licence ouverte « restrictive » : la version N du produit ou service soutenu est ouverte, les développements et versions ultérieurs devront être partagés sous les mêmes conditions de licence

- Le code source est accessible en ligne à tous en lecture dans une version documentée, modifiable et non compressée ;

- Les codes sources livrés sont indépendants d'autres applications logicielles ou leurs dépendances sont en open source répondant aux mêmes conditions d'accès et de licence.

Une architecture multi locataires est en place avec une instance d'application et une base de données unique pour l'ensemble des collectivités.

Le SITIV assure le support de niveau 1 sur cette plateforme, pour toutes les villes.
Le SITIV souhaitant jouer pleinement son rôle d'organisme mutualisant, il souhaite avoir une grande autonomie dans la réalisation de l'ensemble des opérations nécessaires pour exploiter le service pour l'ensemble de ses communes.

Il souhaite que son prestataire de maintenance / développement effectue une mise à jour annuelle de l'ensemble de la plateforme de gestion des identités avec la dernière version

stable de ses composants (LEMONLDAP::NG, OpenLDAP, LSC et LTB Self Service Password) et à cette occasion maintienne les livrables suivants :

• L'application/version/patch
• Le dossier d'architecture technique
•Le dossier d'installation
• Le guide d'exploitation
• Le manuel utilisateur
•Le cahier de recette

Le présent marché a pour objet la maintenance, l'assistance, les études et les développements relatifs à la plateforme de gestion des identités hébergée par le SITIV pour le compte de ses villes adhérentes.
Ce marché inclut également les prestations nécessaires au maintien en condition opérationnelle de la plateforme et au déploiement et à la maintenance de nouveaux développements et/ou de nouvelles villes sur la plateforme existante.

Dans le cadre de ce marché, le SITIV a déjà identifié un certain nombre de nouvelles fonctionnalités qu'il souhaite développer (liste non exhaustive) :

- mise en œuvre d'une identité pivot agent connect territoire et outillage de gestion
- conception d'un portail d'identification présentant les fournisseurs d'identité de la fédération et présentant les applications autorisées
- intégration d'une solution libre d'approvisionnement des identités
- intégration / synchronisation des données SIRH
- mise en œuvre d'un environnement bac à sable

La solution LemonLDAP::NG est en licence libre **GNU General Public License v2.0**. Les sources de l'application sont accessibles via le lien suivant : https://gitlab.ow2.org/lemonldap-ng/lemonldap-ng . Le prestataire démontrera sa capacité à contribuer activement au développement et à la maintenance des fonctionnalités de la solution.

Le maître d'ouvrage du présent appel d'offres est le SITIV. Le prestataire sera l'interlocuteur unique concernant les solutions de mise-en-œuvre.

ARTICLE III. DESCRIPTION DES PRESTATIONS

Dès la notification du marché, le prestataire fait son affaire, sous 5 jours ouvrés, de l'ensemble des opérations d'état des lieux et de prise en main de l'installation du logiciel. Le maintien en condition opérationnelle doit être effectif dès que cette opération sera effectuée.
Pour l'ensemble des bons de commandes liés à la mise en œuvre de nouvelles fonctionnalités et/ou d'équipement de nouvelles collectivités, le délai des prestations est de 6 mois.
Pour les prestations de maintenance et de maintien en conditions opérationnelles, les délais sont définis par l'article II.4.

Section III.1 Nouveaux développements

Le SITIV souhaite être en mesure de développer avec la plateforme LemonLDAP::NG le socle de l'identité de territoire de son bureau virtuel Agent / Elu.

Il aura besoin pour ce faire d'études techniques complémentaires, d'intégration de nouvelles solutions libres à la plateforme, de développements complémentaires.

Le prestataire décrira les conditions dans lesquels il lui est possible de maintenir et de faire évoluer la solution LemonLDAP::NG.

Section III.2 Maintenance et maintien en condition opérationnelle

Dès la première année, et pour l'ensemble de la durée du marché, le titulaire accompagne le SITIV dans l'exploitation de la plateforme en production.

- Assurer la maintenance applicative de la plateforme :
  - Mettre à jour les composants applicatifs
  - Installer les mises à jour de sécurité autant que nécessaire
  - Installer une fois par an une version majeure sur la nouvelle plateforme créée sans coupure d'exploitation en heures ouvrées supérieure à 8 heures
  - Assurer le transfert de compétence au différentiel de version aux administrateurs du SITIV et des villes
  - Fournir les supports de communication personnalisés présentant les principales nouveautés

- Assurer son maintien en condition opérationnelle :
  - Assurer l'ensemble de conseil nécessaire aux administrateurs du SITIV pour assurer l'exploitation de la plateforme
  - Intervenir sur toute forme d'incident d'exploitation non résolu par le SITIV et rétablir le service en moins de 8 heures ouvrées (GTR)
  - Auditer régulièrement le fonctionnement de la plateforme et préconiser les actions préventives de paramétrages et de mise à niveau (1 audit annuel minimum). Cet audit donnera lieu à la rédaction et à la fourniture d'un rapport détaillé d'historique d'exploitation et d'incidents et à la préconisation de solutions d'améliorations et de corrections. Ce rapport sera présenté aux exploitants du SITIV et des villes.

(a) Engagement de délais pour la maintenance

On appelle **anomalie bloquante**, une indisponibilité pendant une longue période ou par rapport à un nombre important d'usagers, du fait du titulaire, du logiciel ou d'une fonction majeure du logiciel ou une anomalie de performances entrainant une indisponibilité du fait du titulaire, du logiciel ou d'une fonction majeure du logiciel. Certaines demandes d'assistance peuvent être considérés comme bloquantes.

On appelle **anomalie majeure**, une indisponibilité partielle pendant une période restreinte ou par rapport à un nombre limité d'usagers, du fait du titulaire, d'une fonction majeure ou une anomalie de performance entrainant une indisponibilité partielle, du fait du titulaire, d'une fonction majeure du logiciel. Certains tickets d'assistance sont considérés comme majeurs.

On appelle **anomalie mineure**, les cas d'anomalies survenant du fait du titulaire et n'entrant ni dans la catégorie des anomalies bloquantes, ni dans la catégorie des anomalies majeures.

Le tableau ci-après décrit les délais maximums à respecter :

Priorité de la demande	Délai de prise en charge	Délai maximum de résolution
Bloquante	1h	8h ouvrées
Majeure	4h	2 jours ouvrés
Mineure	2 jours ouvrés	5 jours ouvrés

Le délai de résolution est calculé entre :

- l'ouverture du ticket horodatée dans l'outil de gestion des tickets proposé par le titulaire ;
- la clôture du ticket par le SITIV après résolution du problème ou réalisation de l'évolution demandée.

Lorsque l'élément réparé redevient indisponible pour les mêmes motifs, la durée d'indisponibilité court depuis le signalement de l'anomalie initiale.

Section III.3 Aspects techniques

La solution actuelle est installée sur les environnements matériels du SITIV.

Le titulaire se charge d'effectuer l'ensemble des opérations de maintien en condition opérationnelle de la plateforme existante.

Le candidat maintiendra l'ensemble des procédures d'installation et d'exploitation (installation d'un serveur, gestion des sauvegardes restauration, surveillance périodique, etc.).

Le titulaire assistera le SITIV dans la mise en œuvre de la solution de supervision de la plateforme en mettant à disposition les différentes caractéristiques techniques des composants à superviser.

ARTICLE IV.RGPD - RGS – RGI – RGAA - PSSI

- **RGPD Règlement Général sur la Protection des Données**

Le règlement européen sur la protection des données a été définitivement adopté par le Parlement européen le 14 avril 2016. Ses dispositions seront directement applicables dans l'ensemble des 28 États membres de l'Union Européenne à compter du 25 mai 2018.
Les 5 grands principes des règles de protection des données personnelles sont les suivants :

- **Le principe de finalité** : le responsable d'un fichier ne peut enregistrer et utiliser des informations sur des personnes physiques que dans un but bien précis, légal et légitime ;
- **Le principe de proportionnalité et de pertinence** : les informations enregistrées doivent être pertinentes et strictement nécessaires au regard de la finalité du fichier ;
- **Le principe d'une durée de conservation limitée** : il n'est pas possible de conserver des informations sur des personnes physiques dans un fichier pour une durée indéfinie. Une durée de conservation précise doit être fixée, en fonction du type d'information enregistrée et de la finalité du fichier ;
- **Le principe de sécurité et de confidentialité** : le responsable du fichier doit garantir la sécurité et la confidentialité des informations qu'il détient. Il doit en particulier veiller à ce que seules les personnes autorisées aient accès à ces informations ;
- **Les droits des personnes**

Concernant le droit des personnes, il est prévu :
- Un consentement « explicite » et « positif » de la part des citoyens.
- Le droit à l'effacement (version allégée du droit à l'oubli) : la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais pour 6 motifs (article 17).
- Le droit à la portabilité des données personnelles : les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement.
- Le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire (article 22 du Règlement).
- Des principes de « protection des données dès la conception » et de « sécurité par défaut » : le règlement européen définit le principe de « protection des données dès la conception » qui impose aux organisations de prendre en compte des exigences relatives à la protection des données personnelles dès la conception des produits, services et systèmes exploitant des données à caractère personnel. De plus, le règlement consacre la nouvelle règle de la

« sécurité par défaut » qui impose à toute organisation de disposer d'un système d'information sécurisé (article 25 du Règlement).
- Des notifications en cas de fuite de données

L'importance des sanctions oblige les collectivités à la prudence : le RGPD donne aux régulateurs le pouvoir d'infliger des sanctions financières allant jusqu'à 4 % du chiffre d'affaires mondial annuel d'une entreprise ou 20 millions d'euros (le montant le plus élevé étant retenu), en cas de non-respect (article 83.6 du Règlement).

Dans ce cadre, le prestataire devra prendre en compte toutes les mesures nécessaires à l'application du Règlement général sur la protection des données (RGPD) et de ses évolutions.
Il tient à la disposition des responsables de traitement le registre tenu par écrit de toutes les catégories d'activités de traitement effectuées pour leur compte conformément aux obligations prévues par le Règlement européen sur la protection des données.
Le titulaire fournit toute l'assistance nécessaire au responsable de traitement pour la réalisation d'analyses d'impact relatives à la protection des données et s'engage à décrire ce qu'il met en œuvre pour permettre aux collectivités de respecter les obligations du RGPD et les droits des personnes concernées : proportionnalité, minimalisation (s'assurer que seules les données pertinentes sont saisies), limitation de la conservation des données, mise à disposition d'une traçabilité des opérations,…

- **RGS Référentiel Général de Sécurité**

Suite au décret numéro 2010-112 du 02 février 2010 et de l'arrêté RGS publié au Journal Officiel le 18 mai 2010, l'application doit respecter les contraintes imposées par le référentiel général de sécurité (RGS) étendu aux utilisateurs des collectivités.
Ce respect doit s'appliquer tant à l'accès à l'application qu'au stockage des données.
Une étude des risques devra être proposée par le candidat couvrant tous les aspects sécurités de son application.
La procédure d'homologation sera ensuite réalisée par le SITIV. Suite aux conclusions rendues par la commission d'homologation du SITIV, le candidat devra se mettre en conformité. A minima, les critères suivants seront vérifiés :
- Liaison HTTPS (échanges sécurisés entre les utilisateurs et la plate-forme)
- Cryptage des mots de passe en base de données
- Utilisation de certificats homologués RGS

Pour obtenir des informations plus poussées sur la sécurité des systèmes d'information, le soumissionnaire peut consulter le site de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

- **RGI – Référentiel Général d'Interopérabilité**

Le RGI est un cadre de recommandations référençant des normes et standards qui favorisent l'interopérabilité au sein des systèmes d'information de l'administration. Ces recommandations constituent les objectifs à atteindre pour favoriser l'interopérabilité. Elles permettent aux acteurs cherchant à interagir et donc à favoriser l'interopérabilité de leur système d'information, d'aller au-delà de simples arrangements bilatéraux.
Toutes les informations de référence sont disponibles sur le site
Le SITIV se servira de ces informations comme référentiel lors de la vérification d'aptitude.

- **RGAA – Référentiel Général d'Amélioration de l'Accessibilité**

Le référentiel général d'accessibilité pour les administrations repose sur les 4 grands principes d'un site internet ou intranet accessible :
- Un site perceptible
- Un site utilisable
- Un site compréhensible
- Un site robuste

Pour chaque outil, le titulaire devra fournir sa déclaration de conformité au RGAA V4.1 minimum et son éventuelle stratégie de mise en conformité, conformément aux exigences de l'article 47 de la loi 2005-102 du 11 février 2005.

Toutes les informations de référence sont disponibles sur le site https://www.numerique.gouv.fr/publications/rgaa-accessibilite/obligations/.

P.S.S.I. – Politique de sécurité du système d'information (SITIV)

Conformément à la PSSI mutualisée avec les villes adhérentes du SITIV, la confidentialité et l'intégrité des flux en interaction avec les systèmes d'information du SITIV doivent respectés les conditions de sécurités suivantes :
Tous les flux d'administration doivent être chiffrés par des procédés fiables (SSH, SSL, Ipsec,etc.), garantissant la confidentialité et l'intégrité des données. De façon générale, tous les flux contenant des informations sensibles et circulant sur un réseau public doivent être chiffrés par des procédés apportant ces mêmes garanties. Le choix et le dimensionnement des algorithmes cryptographiques doivent être effectués conformément aux règles et recommandations du RGS en la matière. Le titulaire indiquera l'ensemble des mécanismes et mesures mis en œuvre pour garantir la confidentialité et l'intégrité des flux d'administration.

ARTICLE V. LOIS, REGLEMENTS ET NORMES

Le titulaire veillera à respecter les lois et règlements qui s'appliquent dans le cadre de l'exercice de sa mission, en aucun cas ne devra contrevenir à ceux-ci et il devra notamment veiller respecter la réglementation et ses évolutions.