



**MINISTÈRES
AMÉNAGEMENT
DU TERRITOIRE
TRANSITION
ÉCOLOGIQUE**

*Liberté
Égalité
Fraternité*

**Secrétariat général
Direction des affaires financières
Direction du Numérique**

ANNEXE 5 au règlement de la consultation

CADRE DE RÉPONSE TECHNIQUE

« Prestation de Bureau d'enregistrement de nom de domaine DNS et d'hébergement sécurisé de zones DNS »

Procédure :SG-SAD3-009-25

SOMMAIRE

Table des matières

1- PRESTATIONS	3
1.1- Les prestations générales	3
1.1.1- Prestations de bureau d'enregistrement	3
1.1.2- Hébergement des zones DNS sur des serveurs faisant autorité	3
1.1.3- Fourniture d'une interface WEB de gestion	4
1.2- Le support	6
1.3- Expertise	7
1.4- La réversibilité	7
2- LA SECURITE	7
2.1- Sécurisation de l'hébergement	7
2.2- Sécurisation des échanges de zone entre le primaire situé dans le centre serveur de la personne publique et les secondaires situés dans le centre serveur du bureau d'enregistrement	10
2.3- Sécurisation de l'accès à l'interface WEB	10
2.4- Mise en œuvre de DNSSEC pour les zones le nécessitant	11
2.5- Conformité aux bonnes pratiques concernant les systèmes DNS (Références : fiches ANSSI)	11
2.6- Audit du centre serveur du bureau d'enregistrement	12
3- PRISE EN COMPTE DU DEVELOPPEMENT DURABLE	12

1- PRESTATIONS

Nota : les informations précisées dans ce chapitre par le candidat seront utilisées pour le jugement du critère n°1 de sélection de l'offre économiquement la plus avantageuse.

1.1- Les prestations générales

1.1.1- Prestations de bureau d'enregistrement

Accréditations

Veuillez indiquer le numéro d'accréditation ICANN de la société.

Si le bureau d'enregistrement possède d'autres accréditations ou est membre actif dans d'autres organisations traitant de la gestion des noms de domaine, il pourra également les faire figurer dans ce paragraphe.

Prestations du bureau d'enregistrement :

- Création, suppression des noms de domaine et mise à jour des informations Whois ;
- Migration d'un portefeuille complet de noms de domaine ;
- Gestion des verrous de niveau registre ;
- Gestion des verrous de niveau bureau d'enregistrement ;
- Gestion du bon renouvellement des noms de domaine ; un mode « renouvellement automatique » doit être possible (fonctionnement par défaut) ;
- Prise en charge des procédures de transfert des noms de domaine (transfert de propriété, transfert de registraire) ;
- Prise en charge de la procédure de « Backorder » pour un nom de domaine non disponible (récupération automatique dès disponibilité et commande différée)
- Conseil sur notre politique de réservation.

Veuillez décrire précisément dans ce paragraphe l'ensemble des procédures permettant la réalisation de ces prestations.

Veuillez fournir la liste des TLD gérés par le bureau d'enregistrement.

Veuillez fournir la liste des registres qui offrent la fonctionnalité de verrou « niveau registre »

1.1.2- Hébergement des zones DNS sur des serveurs faisant autorité

L'hébergement d'une zone DNS peut faire l'objet de trois solutions différentes :

Solution n°1 (la plus fréquente) : La personne publique héberge, sur son centre serveur, le serveur DNS primaire de la zone. Le bureau d'enregistrement héberge la zone sur au moins deux de ses serveurs secondaires.

Solution n°2 : Le bureau d'enregistrement héberge, sur son centre serveur, les serveurs primaire et secondaires de la zone.

Solution n°3 : La personne publique héberge, sur son centre serveur, les serveurs primaire et secondaires de la zone.

Veuillez décrire ici, précisément, l'architecture technique d'hébergement (des schémas seront appréciés)

- Architecture réseau (schéma obligatoire)
- Utilisation de la virtualisation

- Système d'exploitation des machines hébergeant les serveurs DNS
- Les logiciels serveurs DNS utilisés

Veuillez confirmer ici la faisabilité des trois solutions d'hébergement et décrivez le mode de fonctionnement dans chacune des solutions (un schéma par solution sera apprécié)

Dans le cadre de la solution n°1, veuillez confirmer ici la faisabilité de l'utilisation de multiple « Hidden Master » avec adresses IP différentes positionnées dans les centre-serveurs de la personne publique (schéma obligatoire).

Dans le cadre des solutions n°1 et 2 le prestataire devra proposer une option d'hébergement en mode « *anycast* » qui permet de lutter contre les attaques en déni de service. Cette option pourra être activée par nom de domaine.

Veuillez décrire précisément l'architecture *anycast* mise en œuvre.

Les salles machines hébergeant les différents serveurs secondaires du bureau d'enregistrement doivent être situées dans **des lieux géographiques différents**.

Veuillez indiquer ici les lieux d'hébergement des machines (adresse des bâtiments qui accueillent les salles machines). La réponse doit être donnée avec et sans l'option « *anycast* ».

Les serveurs secondaires du prestataire doivent **accepter les notifications en provenance du primaire de la personne publique** afin d'accélérer les transferts de zones.

Veuillez confirmer la mise en œuvre de cette fonctionnalité dans le cadre de la solution d'hébergement n°1.

Veuillez préciser le fonctionnement dans le cas d'une architecture type « *anycast* » permettant de lutter contre les dénis de service.

Dans le cadre de la solution n°1, il doit être possible de gérer **des zones DNS « externes »**. Une zone DNS externe est une zone DNS correspondant à un nom de domaine géré par la personne publique mais qui ne correspond pas directement à un nom de domaine acheté chez le registrar titulaire du marché (exemple : sous-zone déléguée). Il sera ainsi possible de profiter de l'architecture de serveurs DNS secondaires en mode « *anycast* » pour ces zones externes.

Veuillez confirmer et décrire précisément la mise en œuvre de cette fonctionnalité dans le cadre de la solution d'hébergement n°1.

Veuillez confirmer que la personne publique est totalement autonome pour gérer la déclaration des zones externes à travers l'interface web du bureau d'enregistrement.

1.1.3- Fourniture d'une interface WEB de gestion

Fonctionnalités obligatoires de l'outil WEB de gestion du portefeuille de nom de domaine

- L'outil doit être multi-utilisateurs. Des droits particuliers (contrôle de l'accès aux différentes fonctionnalités) peuvent être affectés à chaque utilisateur.
- Commande d'un nom de domaine
- Abandon d'un nom de domaine
- Modification des éléments du Whois
- Modification des NS de la zone

- Affichage de statistiques sur les requêtes DNS effectuées par nom de domaine
- Fonctionnalités de gestion des enregistrements dans les zones pour les cas où le serveur primaire de la zone est géré chez le registraire.
- Fonctionnalité de gestion du DNSSEC
- Suivi de l'avancement des différentes procédures
- Traçabilité de l'ensemble des actions

Veuillez fournir une documentation complète de l'outil. Cette documentation devra, entre autre, décrire très précisément chacune des fonctionnalités obligatoires listées ci-dessus. Les aspects traçabilités devront faire l'objet d'un paragraphe particulier où ils seront décrits très précisément. Cette documentation peut être fournie dans un document dédié. La référence au document sera donnée ici dans le cadre de réponse.

Cette interface doit posséder une API REST qui doit permettre les mêmes fonctionnalités obligatoires listées pour l'interface utilisateur.

Veuillez fournir une documentation complète de l'API REST.

L'interface graphique et l'API REST sont-elles développées en interne au bureau d'enregistrement ou en externe.

oui/non et commentaires

1.2- Le support

Support de base

Le niveau de maintenance et de support attendu de la part du titulaire est le suivant :

- Un binôme d'interlocuteurs appartenant au bureau d'enregistrement est désigné comme contact pour la personne publique.
 - Le rôle de ce contact est d'accompagner la personne publique dans l'ensemble des activités concernant le processus de gestion des domaines.
- Un support téléphonique standard doit être disponible du lundi au vendredi (8h30 – 18h30)
 - Le rôle de ce support téléphonique est d'accompagner la personne publique dans l'ensemble des activités concernant le processus de gestion des domaines.

Veuillez décrire ici l'offre pour le support de base du bureau d'enregistrement.
Détaillez précisément les différents délais d'intervention.

Support en dehors des jours ouvrés et heures de bureau

Un service d'astreinte doit être disponible. Il ne concerne que les prestations d'hébergement.

- Disponibilité d'un support d'urgence 24 heures sur 24 et 7 jours sur 7
- Le déclenchement d'une demande de support doit pouvoir être effectuée par mail ou par téléphone.
- Le support d'urgence est utilisé dans les conditions suivantes :
 - Dysfonctionnement constaté sur les équipements du prestataire (réponse DNS non conforme de la part d'un serveur secondaire hébergé chez le prestataire).
 - Impossibilité de joindre les DNS secondaires du prestataire pour une mise à jour urgente dans une zone.

Veuillez décrire ici l'offre pour le support en dehors des jours ouvrés et heures de bureau.
Détaillez précisément les différents délais d'intervention.

Les Curricula Vitae du binôme d'interlocuteur

Veuillez fournir les CVs des personnes constituant le binôme affecté à la personne publique. L'expérience dans la gestion des noms de domaine et le nombre de domaines gérés par chacune des personnes au moment de la réponse à l'appel d'offre devront être clairement exprimés.

Description de l'équipe gestion des incidents

Veuillez décrire l'équipe en place dédiée à la gestion des incidents.
Veuillez décrire vos procédures de gestion d'incident.
Veuillez décrire vos procédures de gestion de crise.

Description de l'astreinte

Veuillez décrire l'équipe en place dédiée à la gestion de l'astreinte.
Veuillez décrire vos procédures de traitement des incidents en astreinte.

1.3- Expertise

Le bureau d'enregistrement doit **fournir de l'expertise** à la personne publique dans le domaine de la gestion des noms DNS. Cette expertise doit couvrir **les aspects techniques et juridiques**.

Veuillez décrire ici précisément l'ensemble des prestations que le bureau d'enregistrement peut fournir sur les aspects techniques et juridiques.

1.4- La réversibilité

En fin de marché, le bureau d'enregistrement transfère à la personne publique l'ensemble des données stockées sur ses serveurs en lien avec les noms de domaine du portefeuille (zones, contacts). Le moyen de transfert doit permettre le chiffrement des données.

Il fournit également la disponibilité des interlocuteurs afin de faciliter le transfert de masse des noms de domaine chez le nouveau bureau d'enregistrement.

Lorsque les transferts sont finalisés, il supprime de ses serveurs toutes les informations qui concernent le pôle ministériel.

Veuillez décrire ici précisément l'ensemble des actions qui sont à mener par le bureau d'enregistrement sortant dans le cadre d'un tel projet de réversibilité.

2- LA SECURITE

Nota : les informations précisées dans ce chapitre par le candidat seront utilisées pour le jugement du critère n°2 de sélection de l'offre économiquement la plus avantageuse

2.1- Sécurisation de l'hébergement

Le bureau d'enregistrement doit avoir élaboré **une politique de sécurité**.

Veuillez fournir la politique de sécurité

Le bureau d'enregistrement doit avoir élaboré **une politique de mise à jour des systèmes**.

Veuillez décrire la politique de mise à jour des systèmes

- Mise à jour des systèmes d'exploitation
- Mise à jour des logiciels permettant d'offrir le service « hébergement de nom de domaine »

Le bureau d'enregistrement doit avoir élaboré **une politique de cloisonnement des réseaux**

Veuillez décrire la politique de cloisonnement des réseaux en indiquant le positionnement des différents services sur chaque zone cloisonnée.

Une architecture sécurisée permettant de **lutter contre les attaques de type DDOS** doit avoir été mise en œuvre.

Veuillez décrire les techniques et l'architecture mises en place pour lutter contre les attaques de type DDOS.

Le bureau d'enregistrement doit avoir mis en place **un SMSI** (Système de management de la Sécurité de l'Information) conforme à **la norme ISO 27001** ou équivalent, et il doit avoir été audité par un tiers dans le cadre d'un processus d'audit formalisé qui lui délivre la certification .. **Le certificat ISO27001 sera fourni directement dans l'enveloppe de candidature.**

Veuillez décrire précisément le périmètre et la politique du SMSI.

CERT internalisé

La présence d'un CERT internalisé à l'entreprise sera considérée comme un plus. Veuillez décrire l'équipe qui constitue ce CERT et l'ensemble de ses missions.

Sécurité physique

Le candidat doit compléter entièrement le tableau ci-dessous. Si d'autres dispositions de sécurité physique sont présentes dans les centre-serveurs du bureau d'enregistrement, elles peuvent être ajoutées et décrites dans ce cadre de réponse.

SÉCURITÉ PHYSIQUE	REPONSE (OUI/NON)	COMMENTAIRES ET PRÉCISIONS
Menaces environnementales et sinistres		
Le centre d'hébergement est-il soumis à une menace environnementale : zone inondable, proximité d'un aéroport, d'une route à grande circulation ou d'un site industriel à risques (zone SEVESO), foudre ?		
Protection contre les incendies		
Des extincteurs manuels adaptés au matériel informatique et télécoms sont-ils installés dans et aux abords des salles d'hébergement ?		
Le centre dispose-t-il d'un système d'extinction automatique d'incendie ? Préciser la technologie		
Les systèmes de détection d'incendie couvrent-ils toute la surface des salles d'hébergement et leurs abords ?		
Le centre dispose-t-il d'un système de détection de dysfonctionnement des détecteurs d'incendie ?		
Le centre dispose-t-il d'un système de détection de dysfonctionnement des systèmes d'extinction automatique d'incendie ?		
Le centre dispose-t-il de personnel habilité à entrer en salle machine et à intervenir sur des incendies, et présent en permanence (24/7) sur le site ?		
Y-a-t-il un contrat de maintenance des dispositifs anti-incendie ? Quelle est la périodicité de contrôle de ces		

équipements ?		
Protection contre le dégât des eaux		
Quelles sont les dispositions prises afin d'éviter un dégât des eaux (intempéries, fuite du dispositif anti incendie, défaut du système d'évacuation des eaux, ...) ?		
Continuité de l'alimentation électrique		
Le centre dispose-t-il d'une double adduction électrique raccordée par des cheminements distincts ?		
Le centre dispose-t-il d'un ou plusieurs générateurs électriques de secours ?		
Le matériel informatique et télécoms est-il protégé par des onduleurs ?		
Les alertes émises par les onduleurs sont-elles supervisées ?		
Y a-t-il un point individuel de défaillance (Single Point Of Failure – SPOF) sur l'alimentation électrique ?		
Continuité des interconnexions télécoms		
Le centre dispose-t-il d'un raccordement à plusieurs opérateurs internet distincts ?		
Y a-t-il un point individuel de défaillance (Single Point Of Failure – SPOF) sur le raccordement télécoms ?		
Le centre dispose-t-il d'un ou plusieurs raccordement (s) à deux centraux distincts d'un même opérateur internet ?		
Continuité de la climatisation		
La salle d'hébergement dans laquelle seront implantés les équipements du ministère est-elle climatisée ?		
Les systèmes de climatisation sont-ils redondés ?		
La température de la salle d'hébergement et du matériel informatique et télécoms est-elle supervisée ?		
La supervision de la température fait-elle l'objet de différents niveaux d'alerte en fonction de seuils prédéfinis ?		
Une procédure est-elle définie en cas de température élevée ?		
Les systèmes de climatisation sont-ils maintenus et contrôlés régulièrement ?		
Contrôle d'accès		

Une zone « accès contrôlé » est-elle définie autour de la salle d'hébergement ?		
Les enceintes de la zone « accès contrôlé » sont-elles sécurisées de manière à prévenir toute intrusion ?		
De quelle manière se fait l'accès à cette zone « accès contrôlé » ?		
Les traces des accès aux salles d'hébergement sont-elles conservées pendant un an ?		
Les enceintes des salles d'hébergement sont-elles sécurisées de manière à prévenir toute intrusion ?		
Les salles d'hébergement sont-elles protégées par des systèmes de détection d'intrusion ?		
Les abords ou l'intérieur des salles d'hébergement sont-ils surveillés en permanence (vidéo surveillance ou gardiennage pendant les heures non ouvrées) ?		
Les postes d'exploitation du centre d'hébergement sont-ils situés dans une zone « accès contrôlé » ?		

2.2- Sécurisation des échanges de zone entre le primaire situé dans le centre serveur de la personne publique et les secondaires situés dans le centre serveur du bureau d'enregistrement.

Authenticité des échanges de zone : Le bureau d'enregistrement doit permettre l'utilisation de TSIG.

Veuillez indiquer les modalités de mise en œuvre de TSIG.
Quelle est la méthode utilisée pour l'échange du secret partagé ?

Authenticité des échanges de zone : Le bureau d'enregistrement devrait permettre l'utilisation de XoT.

XoT n'est pas obligatoire mais sera considéré comme un plus.

Confidentialité des échanges de zone : Le bureau d'enregistrement doit permettre l'utilisation d'un tunnel chiffré entre le centre serveur de la personne publique et le centre serveur du bureau d'enregistrement.

Veuillez confirmer la faisabilité de la mise en œuvre du tunnel chiffré. Le protocole IPSEC sera privilégié.

Veuillez indiquer les contraintes imposées par le bureau d'enregistrement concernant l'établissement de ce tunnel.

Si le bureau d'enregistrement propose d'autres méthodes pour assurer la confidentialité des échanges de zone, il peut les indiquer dans ce paragraphe.

2.3- Sécurisation de l'accès à l'interface WEB

L'accès à l'interface WEB utilise **obligatoirement le protocole HTTPS.**

Veillez confirmer ici l'utilisation de ce protocole.

Un filtrage par adresse IP source doit pouvoir être activé pour l'accès à cette interface. La liste des IP sources autorisées doit être configurable pour chaque utilisateur.

Veillez confirmer la possibilité de mettre en place ces listes de filtrage pour chaque utilisateur. Veillez fournir des copies d'écran de l'interface pour cette fonctionnalité.

Une authentification forte à double facteur doit pouvoir être activée pour l'accès à cette interface (exemple : utilisation de mot de passe à usage unique généré grâce à un objet que l'on possède)

Veillez indiquer précisément quelle est la technologie employée et les procédures associées.

Délégation de l'authentification

Il doit être possible de déléguer l'authentification sur le système d'authentification forte de la personne publique (compatibilité openID connect ou SASL)
Veillez décrire ici la mise en œuvre de cette fonctionnalité.

2.4- Mise en œuvre de DNSSEC pour les zones le nécessitant

La mise en œuvre de **DNSSEC** doit pouvoir être effectuée dans les trois cas de figure suivants :

1. Le primaire est situé dans le centre serveur de la personne publique et les signatures de zone sont effectuées dans le centre serveur de la personne publique.
2. Le primaire est situé dans le centre serveur de la personne publique mais les signatures sont effectuées dans les locaux du bureau d'enregistrement.
3. Le primaire est situé dans les locaux du bureau d'enregistrement et les signatures de zone sont effectuées dans les locaux du bureau d'enregistrement.

Veillez décrire l'architecture technique mise en place dans le centre serveur du bureau d'enregistrement pour le fonctionnement de DNSSEC.

Veillez décrire l'organisation mise en place dans le bureau d'enregistrement pour le fonctionnement de DNSSEC.

Veillez confirmer la faisabilité des trois cas de figure présentés ci-dessus.

Dans le cadre du cas de figure n°1, veuillez décrire précisément la technique utilisée pour transférer les enregistrements de type DS entre le centre serveur de la personne publique et le centre serveur du bureau d'enregistrement.

TLD compatibles DNSSEC

Veillez fournir la liste des TLD gérés par le bureau d'enregistrement pour lesquels DNSSEC est possible.

2.5- Conformité aux bonnes pratiques concernant les systèmes DNS (Références : fiches ANSSI)

Conformité à la fiche de bonne pratique ANSSI « **RECOMMANDATIONS RELATIVES AUX ARCHITECTURES DES SERVICES DNS** »

Cette fiche de bonnes pratiques est récupérable sur le site de l'ANSSI : <https://cyber.gouv.fr/>

Veillez fournir le tableau de conformité de vos architectures DNS par rapport à cette liste de recommandations.

Conformité à la fiche de bonne pratique ANSSI « **BONNES PRATIQUES POUR L'ACQUISITION ET L'EXPLOITATION DE NOMS DE DOMAINE** »

Cette fiche de bonnes pratiques est récupérable sur le site de l'ANSSI : <https://cyber.gouv.fr/>
Veillez fournir le tableau de conformité de vos architectures DNS par rapport à cette liste de recommandations.

2.6- Audit du centre serveur du bureau d'enregistrement

Des **audits du centre serveur du bureau d'enregistrement** peuvent être demandés par la personne publique. Ils peuvent être réalisés par la personne publique, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ou une société autre que le bureau d'enregistrement.

Veillez confirmer la possibilité d'organiser ce type de prestation.
Veillez indiquer les contraintes du bureau d'enregistrement vis-à-vis de ce type de prestation.

3- Prise en compte du développement durable

Nota : les informations précisées dans ce chapitre par le candidat seront utilisées pour le jugement du critère n°3 de sélection de l'offre économiquement la plus avantageuse

Le bureau d'enregistrement dispose ici d'un cadre libre pour exposer l'ensemble des actions menées en faveur de la prise en compte du développement durable en lien avec l'objet du marché ou à ses conditions d'exécution. Les sujets suivants ne sont pas limitatifs :

Pratiques du candidat en terme de :

- écoconception des produits numériques support de l'activité du candidat,
- matériel durable (utilisation de matériels reconditionnés, matériels basse consommation, ...)
- recyclage (DEEE, tri sélectif,...)
- sobriété numérique (réduction des données, sensibilisation des collaborateurs, ...)
- consommation d'énergies vertes (optimisation énergétique, compensation carbone, certificats énergétiques, ...)
- dispositions pour réduire l'impact des déplacements des collaborateurs