



CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES

SG-SAD3-009-25

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

SOMMAIRE

Table des matières

1	OBJET DU MARCHE	3
1.1	Présentation générale	3
1.2	Objet du marché	3
2	CONTEXTE	4
2.1	Les acteurs et les missions	4
3	PRESTATIONS A REALISER	4
3.1	Les prestations générales.....	4
3.1.1	Prestations de bureau d'enregistrement.....	4
3.1.2	Hébergement des zones DNS sur des serveurs faisant autorité	5
3.1.3	Fourniture d'une interface WEB de gestion	5
3.2	La sécurité.....	6
3.2.1	Sécurisation de l'hébergement	6
3.2.2	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	6
3.2.3	Sécurisation de l'accès à l'interface WEB	6
3.2.4	Mise en œuvre de DNSSEC pour les zones le nécessitant.....	7
3.2.5	Audit du centre serveur du bureau d'enregistrement.....	7
3.3	Le support	7
3.4	Expertise	8
3.5	Réversibilité	8

1 OBJET DU MARCHÉ

1.1 Présentation générale

La Direction du Numérique (DNUM) est rattachée au Secrétariat général du pôle ministériel :

- Ministère de l'Aménagement du territoire et de la Décentralisation,
- Ministère de la Transition écologique, de la Biodiversité, de la Forêt, de la Mer et de la Pêche

La direction du numérique est responsable de l'écosystème informatique du pôle ministériel, de sa fiabilisation et de sa résilience. Elle porte l'ambition numérique en en définissant la stratégie et en mettant en œuvre les infrastructures numériques et les systèmes d'information. Elle maintient et développe de nombreux outils tournés vers le public comme vers les agents. Elle accompagne les directions et services du ministère pour l'élaboration, le déploiement, le maintien et l'évolution de leurs produits numériques, ainsi que pour la transformation des politiques publiques liées au numérique. Elle offre son expertise et ses conseils à ses différents partenaires.

Elle assure la veille et la prospective sur les technologies émergentes et conduit les actions d'innovation.

En son sein, la Fabrique numérique assure le rôle d'incubateur de startups d'État. Elle fait partie de la communauté interministérielle beta.gouv.fr

1.2 Objet du marché

Le présent marché a pour objet des prestations de services présentées comme suit :

- prestation de type « Bureau d'enregistrement » des noms de domaine DNS Internet ; les TLD (domaines de premier niveau) les plus utilisés sont « fr., com., org., net., eu., info., re., gp., mq. » ; de nombreux domaines utilisent l'extension « gouv.fr. » ;
- hébergement sécurisé des zones DNS sur des serveurs faisant autorité (secondaires ou primaires) ;
- fourniture d'une interface WEB sécurisée de gestion du portefeuille de noms de domaine (commande, suivi, abandon, gestion des zones et des enregistrements) ;
- signature des zones DNS (DNSSEC)
- assistance et support pour l'ensemble des prestations ;
- expertise et conseil dans le domaine de la gestion des noms de domaine ;
- réversibilité en fin de marché.

Nota : le titulaire du présent marché est également appelé « Le bureau d'enregistrement » dans ce document.

2 CONTEXTE

2.1 Les acteurs et les missions

La gestion des systèmes DNS Internet et Intranet sur les périmètres ministériel et interministériel a été confiée à la Direction du numérique (DNUM).

C'est le **Groupe Opérations** du département Infrastructure et Services (DIS) au sein de la sous-direction Méthodes et Services de Plateforme (MSP) qui a en charge cette mission.

Une partie de l'hébergement des zones DNS est réalisée dans les centres-serveurs interministériels. Ceux-ci sont répartis géographiquement sur deux sites :

- **Site de Paris / La Défense**
- **Site de Toulouse /**

Le groupe Opérations a en charge la conception et le maintien en conditions opérationnelles et de sécurité des plateformes DNS. Ce groupe a également en charge la gestion technique des zones DNS et la gestion administrative des noms de domaine en lien avec le bureau d'enregistrement :

- gestion technique des zones :
 - paramétrage des zones ;
 - hébergement sur un serveur primaire ;
 - sécurisation des échanges entre les serveurs primaires et secondaires ;
 - participation à la sécurisation des échanges avec le bureau d'enregistrement ;
- gestion administrative des noms de domaine :
 - commande de noms de domaine Internet auprès d'un bureau d'enregistrement (création, récupération, « backorder ») ;
 - commande des opérations sur les noms de domaine :
 - transfert de propriété ;
 - transfert de registraire ;
 - mise à jour des informations du « Whois ».

3 PRESTATIONS A REALISER

3.1 Les prestations générales

3.1.1 Prestations de bureau d'enregistrement

- L'accréditation ICANN (Internet Corporation for Assigned Names and Numbers) est obligatoire.
- Le bureau d'enregistrement doit effectuer les prestations suivantes :
 - Création, suppression des noms de domaine et mise à jour des informations Whois ;
 - Migration d'un portefeuille 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.
- Conseil sur notre politique de réservation.

3.1.2 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 (le plus fréquent)** : 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 ;
Le bureau d'enregistrement doit permettre l'utilisation de serveurs SOA masqués (« Hidden Master ») situés dans le centre serveur de la personne publique. Ces « Hidden Master » peuvent être multiples, répartis géographiquement et donc posséder des adresses IP différentes.
 - **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 ;
- 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.
- Les salles machines hébergeant les différents serveurs secondaires du bureau d'enregistrement doivent être situées dans des lieux géographiques différents.
- Les serveurs secondaires du prestataire doivent accepter les notifications en provenance du primaire (Hidden Master) de la personne publique afin d'accélérer les transferts de zones.
- L'architecture du prestataire doit permettre la gestion du DNSSEC (Domain Name System Security Extensions).
- 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.

3.1.3 Fourniture d'une interface WEB de gestion

- Voici la liste des fonctionnalités obligatoires devant être fournies par l'interface 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.
 - L'outil doit pouvoir gérer plusieurs clients avec séparation des portefeuilles de nom de domaines et des valeurs par défaut (serveurs de noms, contacts whois) de chaque client.
 - Commande d'un nom de domaine.
 - Abandon d'un nom de domaine.
 - Positionnement d'un nom de domaine en mode « backorder » (récupération automatique dès disponibilité et commande différée).
 - Modification des éléments du Whois.
 - Modification des NS de la zone.
 - Affichage de statistiques sur les requêtes DNS effectuées par nom de domaine. Les

valeurs fournies par ces statistiques doivent être disponibles à travers une API REST afin d'être consolidées dans les tableaux de bord de la personne publique.

- Fonctionnalités de gestion des enregistrements dans les zones pour les cas où le serveur primaire de la zone est géré chez le registraire.
- Fonctionnalités de gestion du DNSSEC.
- Fonctionnalité d'export de l'ensemble des noms de domaines du portefeuille et des propriétés associées à chaque nom.
- Fonctionnalité d'export des noms de domaine externes et des propriétés associées à chaque nom.
- Suivi de l'avancement des différentes procédures.
- Traçabilité de l'ensemble des actions.
- Présence d'un service WEB (API REST) associé à l'interface graphique permettant d'accéder aux fonctionnalités fournies par l'outil.

3.2 La sécurité

3.2.1 Sécurisation de l'hébergement

- Le bureau d'enregistrement doit avoir élaboré une politique de sécurité.
- Le bureau d'enregistrement doit avoir élaboré une politique de mise à jour des systèmes.
- Le bureau d'enregistrement doit avoir élaboré une politique de cloisonnement des réseaux.
- Une architecture sécurisée permettant de lutter contre les attaques de type DDOS doit avoir été mise en œuvre.
- Les flux d'échange de zone doivent être sécurisés.
- 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, la description précise du périmètre et de la politique de certification sont exigées.
- La présence d'un CERT internalisé à l'entreprise sera considérée comme un plus.

3.2.2 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 ». La possibilité d'utiliser « XoT » 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. On privilégiera l'utilisation d'un VPN IPSEC entre le centre-serveur du Ministère et le centre-serveur du bureau d'enregistrement.

3.2.3 Sécurisation de l'accès à l'interface WEB

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

- Il doit être possible de déléguer l'authentification sur le système d'authentification forte du client (compatibilité openID connect ou SASL)

3.2.4 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 ; Les zones signées doivent pouvoir être transférées sur les serveurs faisant autorité dans le centre-serveur de la personne publique.
 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.
- Le bureau d'enregistrement devra indiquer dans sa réponse la liste des TLD pour lesquelles DNSSEC est possible.

3.2.5 Audit du centre serveur du bureau d'enregistrement

- Des audits du centre serveur du bureau d'enregistrement peuvent être demandés par la personne publique.

3.3 Le support

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

Un support de base

- 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 ;

Un 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.

3.4 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. L'unité d'œuvre d'expertise est également utilisée pour répondre aux questions des auditeurs dans le cadre des audits qui seraient commandés par le ministère comme décrit au chapitre 3.2.5.

3.5 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.

Il n'y a pas d'unité d'œuvre spécifique à la réversibilité.

La réversibilité est incluse dans les prix des prestations figurant au bordereau des prix.