MINISTÈRE
DE L'ECONOMIE,
DES FINANCES
ET DE LA SOUVERAINETE
INDUSTRIELLE ET NUMERIQUE
ljbcrte"
Egalité
Fmtemité

Direction des Affaires juridiques

Prestations de mise en œuvre d'un service de lutte contre le cybersquattage des signes identitaires de l'État français

Cahier des clauses techniques particulières

Numéro de consultation : CA-01-2024-CYBERSQUATTAGE

Procédure de passation : Appel d'offres ouvert

La présent Cahier des Clauses Techniques Particulières comporte 11 pages, numérotés de 1 à 12.

Table des matières

Chapitre I - Présentation générale

Article 1 – Contexte

Les signes identitaires de l'État constituent des cibles particulièrement exposées aux cyberattaques, notamment au cybersquattage, via la réservation de noms de domaine les reprenant ou les imitant de manière illégitime à des fins malveillantes. Les signes identifiant des services grand public pour lesquels les utilisateurs renseignent des informations personnelles sont particulièrement touchés par ce phénomène (ex : fraudes en lien avec le paiement des amendes, le renouvellement de la Carte Vitale, l'achat des vignettes Crit'Air, etc.).

Dans ce contexte, un service interministériel de lutte contre le cybersquattage des identités de l'État a été mis en place depuis début 2022. Ce service repose sur un marché attribué à un prestataire chargé de la surveillance sur Internet des créations de noms de domaine reprenant ou imitant des signes identitaires de l'État. Le prestataire met également en œuvre des actions de suspension ou de blocage des contenus illicites accessibles à partir des noms de domaine détectés. Des actions juridiques complémentaires ou alternatives pour obtenir le transfert ou la suppression des noms de domaine (mises en demeure, procédures alternatives de règlement des litiges, etc.) sont effectuées directement par la DAJ-Mission APIE. En effet, en vertu de l'article 2 du décret n° 2019-1454 du 24 décembre 2019 relatif à la direction des affaires juridiques des ministères économiques et financiers, modifié par le décret n° 2021-264 du 10 mars 2021, la direction des affaires juridiques via la Mission Appui au patrimoine immatériel de l'État (ci-après, « DAJ-Mission APIE ») engage, avec l'accord des administrations civiles de l'État au sens de l'article 2 du décret du 7 mai 2015 modifié portant charte de la déconcentration, des administrations militaires et des forces armées, toute action administrative ou précontentieuse utile à la protection de leurs marques. La DAJ-Mission APIE peut également engager de telles actions en vue de la protection de leurs noms de domaine et plus généralement de leurs signes distinctifs.

Depuis le lancement de ce dispositif, plus de 220 signes identitaires de l'État ont été placés sous surveillance et plus de 2 500 actions de suspension de sites illicites ont été réalisées. Forte de ce succès et convaincue de la nécessité pour l'État de bénéficier d'un tel service, la DAJ-Mission APIE souhaite poursuivre ce dispositif.

Article 2 – Objet du marché

Le présent marché a pour objet la fourniture de prestations de surveillance de noms de domaine et d'actions consécutives à la détection de noms de domaine malveillants, dans le cadre de la mise en œuvre d'un service de lutte contre le cybersquattage des signes identitaires de l'État.

Sont expressément exclues du présent marché, les prestations suivantes :

- La gestion administrative et technique des noms de domaine ;
- Les actions/démarches juridiques ayant pour objectifs la suppression ou la récupération d'un nom de domaine, notamment :
    - Levée d'anonymat ;
    - Procédure de vérification d'éligibilité/de joignabilité du réservataire du nom de domaine ;

- Lettre de mise en demeure/demande de modification du contenu d'un site Internet ;
- Procédures alternatives de résolution des litiges en matière de noms de domaine (dites, procédures PARL), telles que les procédures UDRP, Syreli, etc.

Le présent document, qui constitue le cahier des clauses techniques particulières (dénommé « CCTP »), a pour objet de décrire les prestations attendues et leur niveau d'exigence.

Chapitre II – Détail des prestations à fournir

Les prestations attendues comprennent :

- Volet 1 - Initialisation et tests ;
- Volet 2 - Surveillance ;
- Volet 3 - Actions de suspension de sites illicites ;
- Volet 4 - Suivi des prestations ;
- Volet 5 - Récupération automatique de noms de domaine (« Backorder ») ;
- Volet 6 - Achat anonyme de noms de domaine ;
- Volet 7 - Formation.

Ces prestations sont détaillées ci-après.

Si le Titulaire s'appuie sur les compétences d'un sous-traitant ou d'un cotraitant pour mener à bien l'ensemble des prestations attendues, il devra le déclarer conformément aux articles 9 et 10.3.9 du CCAP et préciser dans son offre :

- Les prestations qui feront l'objet d'une sous-traitance ou d'un groupement ;
- L'organisation et la répartition des tâches afin de garantir le bon déroulement des prestations (modes de sollicitations, modalités opérationnelles d'exécution, mise en relation directe ou non avec le client) ;
- Les modalités contractuelles.

Article 3 – Volet 1 - Initialisation et tests

Définition : Initialisation de la surveillance, à savoir intégration dans l'outil de surveillance du Titulaire d'une liste de vocables déjà surveillés (environ 250 vocables) incluant les paramétrages nécessaires, et la réalisation de tests pour s'assurer de la pertinence des résultats de la surveillance.

UO 01 « Initialisation de la surveillance, à savoir intégration dans l'outil de surveillance du titulaire d'une liste de vocables déjà surveillés (environ 250 vocables) incluant les paramétrages nécessaires, et la réalisation de tests pour s'assurer de la pertinence des résultats de la surveillance, d'une DUREE D'UN MOIS »

Le service de lutte contre le cybersquattage des signes identitaires de l'État ne doit connaître aucune interruption ou difficulté de mise en place à l'occasion de l'entrée en application du présent marché. Pour assurer la continuité du service, une période de chevauchement d'une durée d'un (1) mois calendaire est prévue entre le marché précédent et le présent marché. Pendant ce délai d'un (1) mois calendaire, le Titulaire entrant réalise exclusivement l'initialisation et les tests nécessaires au démarrage de la prestation de surveillance. Ce n'est qu'à l'issue de ce délai que les autres prestations débuteront de manière effective.

3.1 Initialisation

Sur la base de la liste des vocables à surveiller transmise préalablement par l'administration (environ 250 vocables), le Titulaire entrant réalise toutes les démarches administratives et techniques, notamment de paramétrages, nécessaires à l'intégration de ces vocables au sein de son outil de surveillance, afin de s'assurer de la pertinence des résultats détectés. Ce travail d'initialisation de la surveillance est réalisé en concertation avec l'administration, sur la base des conseils techniques du Titulaire entrant et de la connaissance métiers de l'administration en lien avec les vocables à surveiller.

3.2 Tests

Le Titulaire réalise les tests nécessaires afin de vérifier la pertinence des résultats obtenus suite à l'intégration des vocables au sein de son outil de surveillance. Il partage les résultats de tout ou partie de ces tests avec l'administration pour confirmer qu'ils répondent à son besoin. Au besoin, le Titulaire réalise les ajustements nécessaires pour améliorer la pertinence des résultats obtenus. Ce travail d'ajustement est réalisé en concertation avec l'administration, sur la base des conseils techniques du Titulaire entrant et de la connaissance métiers de l'administration en lien avec les vocables à surveiller.

Article 4 – Volet 2 - Surveillance

Définition : Service de surveillance des signes identitaires de l'État français parmi les noms de domaine (conseils, paramétrages, détection, alertes, surveillance de contenu et de configuration de serveurs de messagerie) pour un certain volume de vocables par an, selon le découpage suivant et les possibilités d'ajustement suivantes :

- UO 02 – 1 : Service de surveillance des signes identitaires de l'État français parmi les noms de domaine (conseils, paramétrages, veille et alertes, surveillance de contenu et de configuration de serveurs de messagerie) pour 250 vocables d'une DUREE ANNUELLE ;
- UO 02 – 2 : Service de surveillance des signes identitaires de l'État français parmi les noms de domaine (conseils, paramétrages, veille et alertes, surveillance de contenu et de configuration de serveurs de messagerie) pour 300 vocables d'une DUREE ANNUELLE ;
- UO 02 – 3 : Service de surveillance des signes identitaires de l'État français parmi les noms de domaine (conseils, paramétrages, veille et alertes, surveillance de contenu et

de configuration de serveurs de messagerie) pour 350 vocables d'une DUREE ANNUELLE ;

- UO 02 – 4 : Service de surveillance des signes identitaires de l'État français parmi les noms de domaine (conseils, paramétrages, veille et alertes, surveillance de contenu et de configuration de serveurs de messagerie) pour 400 vocables d'une DUREE ANNUELLE ;
- UO 02 – 5 : Ajout de 10 vocables à surveiller d'une DUREE MENSUELLE ;
- UO 02 – 6 : Ajout de 20 vocables à surveiller d'une DUREE MENSUELLE ;
- UO 02 – 7 : Ajout de 50 vocables à surveiller d'une DUREE MENSUELLE ;
- UO 02 – 8 : Ajout de 100 vocables à surveiller d'une DUREE MENSUELLE.

La prestation de surveillance permet de détecter la création de noms de domaine reproduisant ou imitant un ou des signes identitaires de l'État dont la liste est fournie par l'administration et complétée/ajustée par l'administration tout au long du marché.

La prestation de surveillance comprend :

- Le conseil ;
- Le paramétrage ;
- La détection ;
- Les alertes ;
- La surveillance de l'évolution du contenu associé aux noms de domaine et de la configuration de serveurs de messagerie.

4.1 Conseil

Le Titulaire assure une mission de conseil à l'égard de l'administration en matière de lutte contre le cybersquattage des signes identitaires de l'État.

Le Titulaire doit ainsi mettre à profit de l'administration son expertise en termes de cybersquattage et de surveillance de noms de domaine.

4.2 Paramétrage

Le Titulaire paramètre son outil de surveillance pour chacun des vocables placés sous surveillance afin d'optimiser la pertinence des résultats obtenus, l'objectif étant de fournir à l'administration des résultats exhaustifs en excluant les résultats non pertinents. Les fonctionnalités de paramétrage sont déterminées par le Titulaire et peuvent notamment inclure l'utilisation de mots-clés, de synonymes, l'ajout ou l'exclusion de termes, etc.

Tout au long du marché, le Titulaire adapte le paramétrage de son outil de surveillance pour chacun des vocables placés sous surveillance afin d'assurer le maintien dans le temps de la pertinence des résultats obtenus et d'optimiser la précision de la surveillance.

La Titulaire travaille en concertation avec l'administration pour optimiser et affiner le paramétrage de la surveillance sur les vocables.

4.3 Détection

La surveillance doit permettre de détecter les noms de domaine nouvellement enregistrés reproduisant ou imitant, sur le plan orthographique, lexical ou intellectuel le cas échéant, au sein d'un nom de domaine un vocable correspondant à un signe identitaire de l'État, y compris avec des variantes telles que :

- des caractères spéciaux ;
- des homoglyphes ;
- d'autres alphabets ;
- des modifications orthographiques ;
- des modifications ortho-phonétiques ;
- etc.

La surveillance mise en place par le Titulaire doit permettre de couvrir l'ensemble des extensions génériques (gTLDs), de pays (ccTLDs) ainsi que les nouvelles extensions (nTLDs) rendues accessibles par les registres. Le Titulaire veillera dans son offre à préciser le périmètre exact de la surveillance proposée.

4.4 Alertes

Le Titulaire doit mettre en œuvre une procédure d'alertes, permettant d'informer l'administration de la détection de noms de domaine reprenant ou imitant un ou des signes identitaires de l'État et lui fournir l'ensemble des informations nécessaires à la détermination des démarches/actions pertinentes à mener à l'égard de ces noms de domaine et/ou des sites Internet accessibles à partir de ceux-ci.

La procédure d'alerte doit comprendre les étapes suivantes :

1. La détection d'un nom de domaine ;
2. La qualification du niveau de menace représenté par le nom de domaine ;
3. La transmission de l'alerte à l'administration.

L'alerte doit, a minima, comporter les éléments d'informations suivants :

- les données issues de la fiche WhoIs du nom de domaine ;
- la copie écran horodatée du site Internet, si existant ;
- la présence ou non d'un serveur de messagerie ;
- la présence ou non d'une redirection.

Le Titulaire doit met en œuvre des critères d'analyse pour qualifier les noms de domaine détectés, a minima en fonction des trois niveaux de menace ci-dessous :

- Absence de menace : nom de domaine présentant une criticité faible ;
- Menace potentielle : nom de domaine présentant une criticité moyenne ;
- Menace avérée : nom de domaine présentant une criticité forte et devant être traité en urgence.

Le Titulaire doit faire apparaître clairement au sein des alertes le niveau de menace pour chacun des noms de domaine détectés. En cas de détection d'un nom de domaine appartenant à l'administration ou supposé lui appartenir, le Titulaire devra faire apparaitre clairement au sein de l'alerte qu'il semble s'agir d'un nom de domaine « officiel/légitime ».

La qualification de la menace liée à un nom de domaine réalisée par le Titulaire au sein de l'alerte est une analyse de premier niveau, qui fera l'objet d'une analyse complémentaire et pourra toujours être modifiée par l'administration.

La périodicité des alertes doit dépendre du niveau de menace identifié :

- Pour les menaces potentielles, la périodicité des alertes doit être hebdomadaire ;
- Pour les menaces avérées, la périodicité des alertes doit être quotidienne afin de permettre une réaction rapide.

Les alertes, quel que soit le degré de menaces, devront en tout état de cause être adressées à l'administration les jours ouvrés sur la plage horaire : 9h00 – 18h00.

Les alertes doivent inclure des recommandations relatives aux actions de suspension de sites illicites pouvant, le cas échéant, être mises en œuvre par le Titulaire.

4.5 Surveillance de contenu et de configuration de serveurs de messagerie

Le Titulaire doit disposer d'un outil de surveillance permettant de détecter les évolutions liées aux noms de domaine considérés comme des menaces avérées dont, a minima :

- L'apparition d'un contenu sur un nom de domaine inactif ;
- Les modifications sur le contenu des sites Internet accessibles via les noms de domaine surveillés ;
- La configuration de serveurs de messagerie.

La périodicité et les modalités de transmission des résultats de la surveillance des évolutions liées aux noms de domaine devront être déterminées en concertation avec l'administration lors de la réunion de lancement (cf. article 10 du présent CCTP).

La surveillance de l'évolution du contenu des sites Internet et de la configuration des serveurs de messagerie doit être mise en place par défaut par le Titulaire pour les noms de domaine remontés sous les qualifications de « menace potentielle » et « menace avérée ».

Pour les noms de domaine remontés sous d'autres qualifications de menace, l'administration peut solliciter auprès du Titulaire la mise en place d'une telle surveillance en spécifiant les évolutions à surveiller.

Concernant la surveillance des évolutions liées aux noms de domaine remontés, le Titulaire devra, dans la mesure du possible, ne faire remonter à l'administration que les évolutions susceptibles d'être pertinentes au regard de l'évaluation du niveau de menace représenté par le nom de domaine et de la détermination des éventuelles actions/démarches pertinentes à engager à son encontre.

Le Titulaire doit également s'assurer que cette surveillance soit susceptible de détecter un contenu accessible à partir d'un nom de domaine, quel que soit le support de visualisation de celui-ci (ordinateur ; téléphone portable ; tablette).

Article 5 – Volet 3 : Actions de suspension de sites illicites

Définition : Service de suspension de sites illicites, avec le découpage suivant et les possibilités suivantes d'ajustement :

- UO 03 – 1 : 1000 actions de suspension de sites illicites sur une DUREE ANNUELLE.
- UO 03 – 2 : Ajout de 20 actions de suspension de sites illicites d'une DUREE MENSUELLE.
- UO 03 – 3 : Ajout de 50 actions de suspension de sites illicites d'une DUREE MENSUELLE.
- UO 03 – 4 : Ajout de 100 actions de suspension de sites illicites d'une DUREE MENSUELLE.

Le Titulaire doit disposer d'une expertise en matière d'actions permettant la suspension des sites illicites (« takedown ») et la mettre à profit de l'administration.

En cas de menace avérée considérée comme critique et/ou récurrente, le Titulaire et l'administration peuvent décider de mettre en place des modalités de systématisation des demandes de suspension des sites illicites.

En parallèle de l'introduction d'une demande de suspension d'un site illicite auprès du bureau d'enregistrement et/ou de l'hébergeur et s'il le juge pertinent, le Titulaire peut également signaler ce même site aux bases anti-phishing, telles que « Google Safe Browsing » ou en demander le déréférencement auprès des moteurs de recherche. Si l'administration le juge nécessaire, elle est également susceptible de demander expressément au Titulaire d'effectuer un signalement auprès des bases anti-phishing et/ou une demande de déréférencement auprès des moteurs de recherche. Ces actions relèvent de la démarche plus générale de suspension du site illicite.

Article 6 – Volet 4 : Suivi des prestations

Définition : Suivi des prestations via :

- UO 04 : Fourniture d'un outil de communication des résultats des prestations et leurs suivis d'une DUREE ANNUELLE.

Le Titulaire doit mettre en œuvre l'ensemble des moyens utiles et nécessaires pour communiquer à l'administration, selon la périodicité déterminée en concertation avec l'administration, les résultats de la prestation et leurs suivis, en tenant compte des éventuelles contraintes de l'administration en termes de sécurité (ex : dispositifs antivirus de messagerie susceptibles de bloquer des mails ou leurs annexes comportant des URLs suspectes). L'outil de suivi du Titulaire doit ainsi inclure un système de notification par email tenant compte de la contrainte précitée.

Le Titulaire doit mettre à disposition de l'administration les résultats de la surveillance, les alertes ainsi que les informations relatives au suivi des actions de suspension de sites illicites sur un outil accessible au travers d'un navigateur web permettant la consultation de ces éléments, le suivi de leurs traitements en temps réel, notamment en cas de demandes de suspension de sites illicites, mais également la transmission d'informations/d'instructions de l'administration vers le Titulaire et inversement. Tout au long du marché, le Titulaire met en œuvre les moyens nécessaires pour garantir à l'administration l'accès à cet outil en termes de qualités techniques, régularité, sécurité et confidentialité des données transmises via l'outil et le bon fonctionnement des fonctionnalités précitées.

L'outil de communication doit être accessible sur la plage horaire : 9h00 – 18h00.

L'hébergement, l'exploitation et l'administration technique de cet outil sont à la charge du Titulaire. L'interface de l'outil ainsi que l'ensemble des échanges réalisés au travers de l'outil doivent être en langue française.

L'outil doit permettre de réaliser des rapports rédigés en langue française et exportables, a minima, sous format PDF et Excel, sur les alertes en cours ou passées, la liste des vocables sous surveillance ainsi que les actions de suspension de sites illicites.

L'outil doit inclure une fonctionnalité permettant de réaliser des recherches d'informations ou d'alertes, de trier ou filtrer selon, a minima, les critères suivants :

- Les vocables surveillés ;
- Les noms de domaine remontés ;
- Les ministères concernés par les vocables surveillés ;
- La qualification de l'alerte ;
- Le type d'atteinte ;
- La date de détection de l'alerte ;
- Le statut de l'alerte ;
- La date de lancement de l'action de suspension du site illicite et sa date de suspension effective.

L'outil doit également permettre à l'administration de générer en autonomie des indicateurs par vocables, par groupe de vocables ou par types de fraudes.

Article 7 – Volet 5 : Récupération automatique de noms de domaine (« backorder »)

Définition : Service de récupération automatique de noms de domaine ("backorder"), selon les modalités suivantes :

- UO 05 – 1 : Service de récupération automatique de noms de domaine ("backorder") pour 1 nom de domaine ;
- UO 05 – 2 : Service de récupération automatique de noms de domaine ("backorder") pour 5 noms de domaine.

Le Titulaire doit proposer un service de récupération automatique de noms de domaine retombant dans le domaine public.

Article 8 – Volet 6 : Service de rachat anonyme de noms de domaine

Définition : Service d'achat anonyme de noms de domaine, selon les modalités suivantes :

- UO 06 – 1 : Service d'achat anonyme de noms de domaine pour 1 nom de domaine ;
- UO 06 – 2 : Service d'achat anonyme de noms de domaine pour 5 noms de domaine.

Le Titulaire doit proposer un service d'accompagnement au rachat anonyme de noms de domaine, incluant la prise de contact anonyme avec le réservataire du nom de domaine, la

représentation anonyme de l'administration dans les négociations, la sécurisation de la transaction ainsi que le transfert du nom de domaine vers l'administration.

Article 9 – Volet 7 : Formation

Définition : Session de formation, initiale ou complémentaire, aux outils du Titulaire, en présentiel ou en distanciel, à destination des agents du bureau juridique de la DAJ/Mission APIE et élaboration d'une documentation pédagogique pour l'utilisation des outils du Titulaire, selon les modalités suivantes :

- UO 07 – 1 : Session de formation aux outils du Titulaire, en présentiel ou en distanciel, à destination de 10 à 15 agents du bureau juridique de la DAJ/Mission APIE ;
- UO 07 – 2 : Elaboration d'une documentation pédagogique pour l'utilisation des outils du Titulaire.

9.1 Sessions de formation

Au lancement de la prestation, le Titulaire doit organiser et dispenser une session de formation sur les outils qu'il mettra à disposition de l'administration. Cette session de formation se déroulera, en distanciel, auprès de 10 à 15 agents de l'État.

En cas d'évolution de ses outils, le Titulaire doit proposer à l'administration et organiser une session de formation complémentaire sous le même format.

En cas de besoin, notamment l'arrivée de nouveaux agents au sein de l'équipe dédiée à ce dispositif, l'administration pourra solliciter du Titulaire de nouvelles sessions de formation.

9.2 Documentation

Au lancement de la prestation, le Titulaire doit fournir un support de type « guide pour les utilisateurs » (au format numérique) détaillant les fonctionnalités des outils qu'il mettra à disposition de l'administration.

Le Titulaire actualise régulièrement ce guide afin qu'il demeure à jour des éventuelles évolutions/modifications des fonctionnalités de ces outils.

Article 10 - Suivi périodique (comitologie, indicateurs)

Le Titulaire devra organiser une réunion de lancement dans les 5 jours ouvrés suivant la date de notification du présent marché afin de définir le cadre général des prestations ainsi que l'ensemble des exigences attendues de la part de l'administration. Le Titulaire est responsable de la planification de cette réunion de lancement.

Le Titulaire doit fournir des indicateurs de suivi des prestations selon une périodicité qui sera déterminée lors de la réunion de lancement. Le choix des indicateurs pertinents est à déterminer en concertation avec l'administration également lors de la réunion de lancement.

Le Titulaire doit organiser une réunion de suivi à une fréquence, a minima, trimestrielle. Cette réunion doit se tenir à distance ou dans les locaux de l'administration lors d'un jour ouvré. La réunion de suivi est d'une durée comprise entre 2 et 3 heures et positionnée sur une demi-journée (9h30-12h30 ou 14h-17h par exemple si 3 heures sont jugées nécessaires). Le Titulaire

est responsable de la planification de ces réunions de suivi.

Lors des réunions de suivi, le Titulaire doit présenter les indicateurs de suivi et de pilotage de l'activité de service de lutte contre le cybersquattage et faire des propositions sur des axes d'amélioration de la prestation. Ces indicateurs auront été transmis à l'administration préalablement aux réunions de suivi et a minima 5 jours ouvrés avant ces réunions de suivi.

Annuellement, le Titulaire doit présenter une revue complète de l'activité du service de lutte contre le cybersquattage. Cette réunion doit se tenir à distance ou dans les locaux de l'administration lors d'un jour ouvré. La réunion annuelle est d'une durée comprise entre 2 et 3 heures et positionnée sur une demi-journée (9h30-12h30 ou 14h-17h par exemple si 3 heures sont jugées nécessaires). Le Titulaire est responsable de la planification de ces réunions annuelles. Lors des réunions annuelles, le Titulaire doit présenter les indicateurs pour l'année écoulée et faire des propositions sur des axes d'amélioration de la prestation. Ces indicateurs auront été transmis à l'administration préalablement aux réunions annuelles et a minima 5 jours ouvrés avant ces réunions annuelles.

Le Titulaire doit transmettre un compte-rendu de chaque réunion au plus tard 5 jours ouvrés après la réunion et le faire valider auprès de l'administration.

La réalisation des supports de présentation des différentes réunions est à la charge du Titulaire.

La langue française doit être utilisée pour la tenue des réunions et la rédaction des livrables.

En dehors de ces réunions, le Titulaire et l'administration échangent de manière régulière pour assurer un fonctionnement optimal du service.