Version préliminaire du Guide de candidature, v4

Module 5

Notez qu'il s'agit uniquement d'une discussion préliminaire. Les candidats potentiels ne doivent pas s'appuyer sur les détails présentés dans le programme relatif aux nouveaux gTLD, ce programme restant soumis à modification suite aux différents commentaires qui seront reçus.

Ce document a été traduit de l'anglais afin d'atteindre un plus grand public. Si la société pour l'attribution des noms de domaine et des numéros sur Internet (l'ICANN) s'est efforcée de vérifier l'exactitude de la traduction, l'anglais reste la langue de travail de l'ICANN et l'original de ce document, rédigé en anglais, est le seul texte officiel et faisant autorité.

31 mai 2010

Module 5

Transition vers la délégation

Ce module décrit les étapes finales à effectuer par un candidat pour conclure le processus, notamment la définition d'un contrat de registre avec l'ICANN et la préparation pour la délégation de la chaîne des nouveaux gTLD dans la zone racine.

5.1 Contrat de registre

Tous les candidats qui ont réussi le processus d'évaluation, notamment, le cas échéant, les procédures de règlement des différends et de traitement des conflits de chaînes, doivent conclure un contrat de registre avec l'ICANN avant de poursuivre jusqu'à la phase de délégation.

La version préliminaire du contrat de registre peut être révisée dans l'annexe de ce module. Tous les candidats retenus sont censés conclure cet accord tel que cela est indiqué. Il est important de noter que le contrat mentionné ci-dessus ne constitue pas un poste officiel chez l'ICANN et n'a pas été approuvé par son Conseil d'administration. Le contrat dont il est question constitue une version préliminaire définie à des fins d'examen et de discussion au sein de la communauté, et comme un moyen d'améliorer l'efficacité du contrat quant à proposer une concurrence et un choix accrus pour les consommateurs dans un DNS stable et sécurisé.

Avant de conclure un contrat de registre avec un candidat, l'ICANN peut procéder à un examen préalable du contrat. Pour s'assurer qu'un candidat continue à respecter dans la durée les obligations légales, l'ICANN se réserve le droit de lui demander de soumettre une documentation et des informations à jour avant de conclure le contrat de registre. L'établissement de tout contrat de registre par l'ICANN doit d'abord être approuvé par le conseil d'administration de l'ICANN.

Avant ou pendant l'exécution du contrat de registre, le candidat doit également fournir une preuve documentaire de sa capacité à financer des fonctions de registre essentielles pour ses futurs requérants pour une durée de trois à cinq ans en cas de défaillance ou de défaut du registre, ou jusqu'à la désignation d'un nouvel opérateur. Il

est possible de s'acquitter de cette obligation en recourant à un instrument financier (« instrument assurant la continuité des opérations »), comme indiqué dans les critères d'évaluation.

5.2 Test préalable à la délégation

Chaque candidat devra effectuer des tests techniques préalables à la délégation comme étape obligatoire pour la délégation dans la zone racine. Ce test préalable à la délégation doit être effectué dans le délai précisé sur le contrat de registre.

L'objectif du test technique préalable à la délégation est de vérifier que le candidat a honoré son engagement relatif à une gestion du registre conformément aux critères techniques et opérationnels décrits dans le module 2.

Le test permet également d'indiquer que le candidat peut gérer le gTLD de manière stable et sécurisée. Tous les candidats seront testés selon la méthode « réussite/échec », d'après les obligations ci-après.

Les éléments du test couvrent à la fois l'infrastructure opérationnelle du serveur DNS et les opérations du système de registre. Dans la plupart des cas, le candidat effectuera les éléments du test en suivant les instructions et présentera les résultats documentés à l'ICANN de façon à faire preuve de ses performances satisfaisantes. Les aspects de cette documentation d'auto-certification réalisée par le candidat peuvent être audités soit sur site au point de fourniture des services du registre, soit autre part, à la discrétion de l'ICANN.

5.2.1 Procédures de test

Le candidat peut initier le test préalable à la délégation en soumettant à l'ICANN un formulaire de pré-délégation ainsi que les documents à joindre devant comporter l'ensemble des informations suivantes :

- Tous les noms de serveur et adresses IPv4/IPv6 à utiliser pour servir les nouvelles données TLD ;
- Si vous utilisez la technique anycast, la liste des noms et des adresses unicast IPv4/IPv6 permettant l'identification de chaque serveur individuel dans les ensembles anycast ;

- Si l'IDN est pris en charge, les tables d'IDN compètes utilisées dans le système de registres ;

- La nouvelle zone TLD doit être signée au moment du test et l'ensemble de clés valide à utiliser pour le test doit être fourni à l'ICANN avec la documentation, ainsi que la déclaration de politique DNSSEC (DPS) TLD ;

- l'accord exécuté entre le dépositaire légal sélectionné et le candidat et

- La documentation d'auto-certification, telle que décrite ci-dessous pour chaque élément de test.

L'ICANN contrôlera les documents soumis et, dans certains cas, procédera à des tests supplémentaires. Après ces tests, l'ICANN produira un rapport indiquant les résultats des tests et le communiquera au candidat.

Toute demande de clarification ou d'information supplémentaire, ainsi que toute autre demande soulevée lors du processus sera mise en évidence et répertoriée dans le rapport remis au candidat.

L'ICANN peut demander au candidat d'effectuer des tests de chargement en tenant compte d'une charge regroupée, où une entité unique effectue des services de registre pour plusieurs TLD.

Lorsque le candidat a rempli toutes les obligations du test préalable à la délégation, il est éligible à la demande de délégation du gTLD faisant l'objet de la candidature.

Si un candidat n'effectue pas les étapes préalables à la délégation dans le délai précisé dans le contrat de registre, l'ICANN se réserve le droit de résilier ledit contrat.

5.2.2 Éléments du test : infrastructure DNS

Le premier ensemble d'éléments de test concerne l'infrastructure DNS du nouveau gTLD. Lors de tous les tests de l'infrastructure DNS, l'ensemble des conditions requises sont indépendantes de l'utilisation d'IPv4 ou d'IPv6. Tous les

tests doivent être effectués via IPv4 et IPv6, avec des rapports fournissant des résultats selon les deux protocoles.[1]

Prise en charge d'UDP -- L'infrastructure DNS à laquelle ces tests s'appliquent comprend l'infrastructure serveur et réseau dans son intégralité. Elle doit être utilisée par les fournisseurs sélectionnés pour assurer le service DNS sur Internet pour le nouveau gTLD. La documentation fournie par le candidat doit comporter les résultats d'un test de performance du système indiquant les fonctionnalités réseau et serveur disponibles, ainsi qu'une estimation des capacités lors d'un fonctionnement normal attendues afin d'assurer un service stable et d'envoyer de façon adéquate des attaques par déni de service distribuées (Distributed Denial of Service : DDoS).

La documentation d'auto-certification doit comporter des données sur la capacité de charge, la latence et l'accessibilité au réseau.

La capacité de charge doit être rapportée sous la forme d'un tableau accompagné d'un graphique, indiquant le pourcentage de requêtes recevant une réponse par rapport au nombre croissant de requêtes par seconde générées à partir d'un ordinateur local (vers les serveurs) par les générateurs de trafic. Le tableau doit comporter au moins 20 points de données et un nombre important de requêtes basées sur UDP, ainsi que des charges qui causeront jusqu'à 10 % de perte pour les requêtes par rapport à un sous-ensemble de serveurs choisis de manière aléatoire au sein de l'infrastructure DNS du candidat. Les réponses doivent contenir des données de zone ou appartenir aux types de réponses NXDOMAIN ou NODATA pour être considérées comme valides.

La latence de la requête sera exprimée en millisecondes, telle qu'elle est mesurée lors des tests DNS à l'extérieur des routeurs de bordure du réseau physique hébergeant les serveurs de noms, du point de vue de la topologie du réseau.

L'accessibilité sera documentée en fournissant des informations sur le transit et les accords de peering pour les emplacements de serveur DNS, notamment en

[1] Des fonctionnalités IPv6 sont incorporées dans différents domaines de test, contrairement aux versions précédentes, où IPv6 était spécifié comme un élément de test individuel.

répertoriant les numéros AS des fournisseurs ou pairs de transit à chaque point de présence, ainsi que la largeur de bande disponible à ces points de présence.

Prise en charge TCP -- Le service de transport TCP pour les requêtes et les réponses DNS doit être activé et prévu pour la charge attendue. L'ICANN contrôlera la documentation d'auto-certification relative aux capacités fournie par le candidat et procédera à des tests d'accessibilité au TCP et de capacité de transaction à travers un sous-ensemble de serveurs de noms sélectionnés de manière aléatoire au sein de l'infrastructure DNS du candidat. En cas d'utilisation de la technique anycast, chaque serveur individuel de chaque ensemble anycast sera testé.

La documentation d'auto-certification doit comporter des données sur la capacité de charge, la latence et la joignabilité du réseau externe.

La capacité de charge doit être rapportée sous la forme d'un tableau accompagné d'un graphique, indiquant le pourcentage de requêtes recevant une réponse valide (données de zone, NODATA ou NXDOMAIN) par rapport au nombre croissant de requêtes par seconde créées à partir de générateurs de trafic locaux (vers les serveurs de noms). Le tableau doit comporter au moins 20 points de données, ainsi que des charges qui causeront jusqu'à 10 % de perte pour les requêtes (soit en raison d'une expiration de délai de connexion, soit d'une réinitialisation de connexion) par rapport à un sous-ensemble de serveurs choisis de manière aléatoire au sein de l'infrastructure DNS du candidat.

La latence de la requête sera exprimée en millisecondes, telle qu'elle est mesurée lors des tests DNS à l'extérieur des routeurs de bordure du réseau physique hébergeant les serveurs, du point de vue de la topologie du réseau.

L'accessibilité sera documentée grâce à la fourniture d'enregistrements de requêtes DNS transportées via IPv6 à partir de nœuds extérieurs au réseau hébergeant les serveurs. Ces emplacements peuvent être identiques à ceux utilisés pour mesurer la latence, comme indiqué ci-dessus.

Prise en charge DNSSEC -- Le candidat doit prouver qu'il prend en charge EDNS(0) dans son infrastructure serveur, qu'il est capable de renvoyer correctement des

enregistrements de ressource liés à DNSSEC, tels que DNSKEY, RRSIG et NSEC/NSEC3 pour la zone signée, ainsi que la capacité à accepter et publier des enregistrements de ressource DS de la part des administrateurs de domaine de second niveau. Le candidat doit notamment démontrer sa capacité à prendre en charge le cycle de vie complet des clés KSK et ZSK. L'ICANN contrôlera les documents d'auto-certification et testera l'accessibilité, les tailles des réponses et la capacité de transaction DNS pour les requêtes DNS qui utilisent l'extension de protocole EDNS(0) avec l'ensemble de bits « DNSSEC OK » pour un sous-ensemble de tous les serveurs de noms sélectionnés de manière aléatoire au sein de l'infrastructure DNS du candidat. En cas d'utilisation de la technique anycast, chaque serveur individuel de chaque ensemble anycast sera testé.

La capacité de charge, la latence de la requête et l'accessibilité doivent être documentées comme indiqué pour le TCP ci-dessus.

5.2.3 Éléments du test : systèmes de registre

Comme il est documenté dans le contrat de registre, les registres doivent prendre en charge le protocole EPP au sein de leur système d'enregistrement partagé, et fournir le service Whois via le port 43, mais aussi par l'intermédiaire d'une interface Web, en plus de la prise en charge de DNS. Cette section détaille les obligations relatives au test de ces systèmes de registre.

Performances du système -- Le système de registre doit évoluer pour satisfaire les exigences de performance décrites dans la Spécification 6 du contrat de registre et l'ICANN exigera une auto-certification de conformité. L'ICANN contrôlera la documentation d'auto-certification fournie par le candidat pour vérifier le respect de ces exigences minimales.

Prise en charge Whois -- Le candidat doit fournir les services Whois pour la charge prévue. L'ICANN vérifiera l'accessibilité des données Whois à travers IPv4 et IPv6, via le port TCP 43 et l'interface Web, ainsi que la documentation d'auto-certification relative à la prise en charge des transactions Whois. Le format de réponse conformément à la Spécification 4 du contrat de registre et à l'accès à Whois (via le port 43 et l'interface Web) sera

testé à distance par l'ICANN depuis différents points sur Internet, via IPv4 et IPv6.

Les documents d'auto-certification doivent décrire le nombre maximal de requêtes par seconde gérées avec succès par les serveurs du port 43, ainsi que par l'interface Web. Le candidat doit également indiquer une estimation de la charge.

De plus, une description des fonctions de contrôle mises en place pour détecter et limiter l'exploitation de la base de données Whois doit être documentée.

Prise en charge EPP -- Étant impliqué dans un service d'enregistrement partagé, le candidat doit fournir des services EPP pour la charge anticipée. L'ICANN vérifiera la conformité aux RFC adéquats (notamment les extensions EPP pour DNSSEC). L'ICANN contrôlera également la documentation d'auto-certification en ce qui concerne la fonctionnalité de transaction EPP.

La documentation doit indiquer un taux maximal de transactions par seconde pour l'interface EPP avec 10 points de données correspondant aux tailles des bases de données de registres, de 0 (vide) jusqu'à la taille attendue après une année de fonctionnement, déterminée par le candidat.

La documentation doit également décrire les mesures prises pour gérer la charge pendant les opérations de registre initiales, telles que la période de « Land-rush ».

Prise en charge IPv6 -- La possibilité pour le registraire d'ajouter, modifier et supprimer des enregistrements DNS IPv6 fournis dans le registre par les requérants sera testée par l'ICANN. Si le registre prend en charge l'accès EPP via IPv6, il sera testé à distance par ICANN à partir de différents points sur Internet.

Prise en charge DNSSEC -- L'ICANN contrôlera la possibilité pour le registraire d'ajouter, modifier et supprimer des enregistrements de ressource liés à DNSSE dans le registre ainsi que les principales procédures de gestion dans l'ensemble du registre. Le candidat doit notamment démontrer sa capacité à prendre en charge le cycle de vie complet des changements clés pour les domaines enfants. L'interopérabilité des canaux de communication

sécurisés du candidat avec l'IANA pour l'échange de matériel d'autorité de certification sera vérifiée.

Le document sur les pratiques et les politiques (également appelé déclaration de politique DNSSEC ou DPS) décrivant le stockage principal du matériel, l'accès et l'utilisation de ses propres clés et le matériel d'autorité de certification du requérant est également contrôlé lors de cette étape.

Prise en charge IDN -- L'ICANN vérifiera l'intégralité des tables IDN utilisées dans le système de registre. Ces tables doivent respecter les directives définies à l'adresse suivante : http://iana.org/procedures/idn-repository.html.

Les exigences liées aux IDN pour les services Whois sont en cours de développement. Lorsque ces exigences auront été développées, les registres prospectifs devront correspondre à la publication des exigences Whois liées aux IDN dans le cadre du test de pré-délégation.

Remise de dépôt -- Les échantillons de dépôt de données fournis par le candidat, qui incluent un dépôt complet et un différentiel, présentant un type et un format de contenu corrects seront contrôlés. Une attention particulière sera portée au contrat passé avec le fournisseur de dépôt pour s'assurer que les données déposées peuvent être publiées dans les 24 heures en cas d'urgence et que le registre a reconstitué dans un délai d'un jour ouvré le point auquel il peut répondre aux requêtes DNS et Whois (à la fois via le port 43 et l'interface web), si nécessaire. L'ICANN peut, comme option, demander à un tiers indépendant de démontrer l'aptitude à la reconstitution du registre à partir de données de dépôt.

5.3 Processus de délégation

Sur réception de l'avis de réussite des tests préalables à la délégation de l'ICANN, les candidats peuvent entamer le processus requis pour la délégation du nouveau gTLD dans la base de données de la zone racine. Cette opération inclut la disposition d'informations supplémentaires et la réalisation d'étapes techniques supplémentaires requises pour la délégation. Des informations sur le processus de délégation sont consultables sur le site http://iana.org/domains/root/.

5.4 Continuité fonctionnelle

Un candidat étant délégué en tant que gTLD deviendra un « opérateur de registre ». En se voyant déléguer un rôle d'opérateur du système de nom de domaine Internet, le candidat assumera un certain nombre de responsabilités significatives. L'ICANN tiendra l'ensemble des nouveaux opérateurs gTLD pour responsables des performances définies par les obligations du contrat de registre, c'est pourquoi il est important que l'ensemble des candidats comprennent ces responsabilités.

5.4.1 Quelles sont les obligations d'un opérateur de registre

Le contrat de registre définit les obligations qui incombent aux opérateurs de registre gTLD. Le non-respect des obligations qui s'appliquent à l'opérateur de registre peut entraîner des sanctions de la part de l'ICANN pouvant aller jusqu'à la résiliation du contrat de registre. Les candidats prospectifs sont invités à lire la brève description ci-dessous des principales responsabilités.

Attention, il s'agit d'une liste non exhaustive fournie aux candidats potentiels comme une introduction aux responsabilités qui incombent à un opérateur de registre. Pour lire l'intégralité du texte officiel, reportez-vous à la version préliminaire du contrat de registre.

Un opérateur de registre doit respecter les obligations suivantes :

Faire fonctionner le TLD de façon stable et sécurisée. L'opérateur de registre est responsable de l'ensemble des opérations techniques du TLD. Comme indiqué dans la norme RFC 1591 :

« Le gestionnaire désigné doit faire fonctionner de façon satisfaisante le service DNS pour le domaine. En effet, la gestion de l'attribution des noms de domaine, de la délégation des sous-domaines et des serveurs de noms nécessite des compétences techniques. Cela implique de tenir l'IR central[2] (dans le cas des domaines de premier niveau), ou d'autres gestionnaires de domaine de haut niveau, informés du statut du domaine, de répondre

[2] IR est une référence historique au terme « Internet Registry » (Registre Internet), une fonction désormais assurée par l'ICANN.

rapidement aux requêtes et de gérer la base de données avec précision, autorité et endurance. »

L'opérateur de registre est dans l'obligation de se conformer aux standards techniques adéquats, qu'il s'agisse de normes RFC ou d'autres directives. En outre, l'opérateur de registre doit satisfaire aux exigences de performances dans des domaines tels que les temps d'arrêt et les temps de réponse du système (voir la Spécification 6 de la version préliminaire du contrat de registre).

Se conformer aux politiques consensuelles et les politiques provisoires. Les opérateurs de registre gTLD ont l'obligation de se conformer aux politiques consensuelles. Les politiques consensuelles concernent un large éventail de sujets tels que les problèmes affectant l'interopérabilité du DNS, la fonctionnalité du registre et les exigences de performance, la sécurité et la stabilité des bases de données, ou encore le règlement des différends portant sur l'enregistrement des noms de domaine.

Pour être intégrée aux politiques consensuelles, une politique doit être développée par l'organisation de soutien des noms génériques (GNSO)[3] selon le processus décrit dans l'annexe A des statuts de l'ICANN.[4] Le processus de développement des politiques implique la délibération et la collaboration des différents groupes de parties prenantes, ce qui permet au public de participer et de donner son avis. C'est pourquoi ce processus peut prendre un temps important.

La politique de transfert entre bureaux d'enregistrement (qui régit les transferts de noms de domaine entre bureaux d'enregistrement) est un exemple de politique consensuelle existante, tout comme la Procédure d'évaluation des services de registre (qui établit un contrôle des nouveaux services de registre proposés pour des raisons de sécurité, de stabilité ou de compétitivité). Il existe bien d'autres exemples disponibles sur le site http://www.icann.org/en/general/consensus-policies.htm.

Les opérateurs de registre gTLD sont dans l'obligation de se conformer à la fois aux politiques consensuelles existantes et à celles qui seront développées dans le futur. Lorsqu'une

[3] http://gnso.icann.org
[4] http://www.icann.org/en/general/bylaws.htm#AnnexA .

politique consensuelle est formellement adoptée, l'ICANN indique aux opérateurs de registre ce qu'ils doivent mettre en œuvre pour adopter cette nouvelle politique, ainsi que la date de son entrée en vigueur.

En outre, le conseil d'administration de l'ICANN peut, lorsque les circonstances l'exigent, établir une politique temporaire pour préserver la stabilité ou la sécurité des services de registre ou du DNS. Dans une telle situation, l'ensemble des opérateurs de registre gTLD devront se conformer à la politique temporaire pour la durée déterminée.

Pour plus d'informations, reportez-vous à la Spécification 1 de la version préliminaire du contrat de registre.

Mettre en œuvre des mesures de protection des droits de démarrage. L'opérateur de registre doit implémenter, au minimum, soit une période sunrise, soit un service de plaintes concernant les marques commerciales lors des phases de démarrage pour l'enregistrement dans le TLD. Ces mécanismes seront soutenus par Clearinghouse pour les marques, comme indiqué par l'ICANN. La période sunrise permet aux détenteurs de droits éligibles d'enregistrer des noms dans le TLD à un stade précoce. Le service de plaintes concernant les marques commerciales avertit les requérants potentiels de droits existants sur les marques commerciales. Il avertit également les détenteurs de droits concernant les noms pertinents enregistrés. Les opérateurs de registre peuvent continuer de proposer le service de plaintes concernant les marques commerciales une fois les phases de démarrage appropriées terminées. Pour plus d'informations, voir la Spécification 7 de la version préliminaire du contrat de registre et le modèle Clearinghouse pour les marques accompagnant ce module.

Mettre en œuvre après lancement des mesures de protection des droits. L'opérateur du registre doit implémenter des décisions prises avec la procédure de suspension rapide uniforme, y compris la suspension de noms de domaine spécifiques au sein du registre. L'opérateur de registre est également tenu de respecter et de mettre en œuvre les décisions prises selon la politique de règlement des différends après délégation (PDDRP) de la marque. Les mesures requises sont décrites en détail dans les procédures de suspension rapide uniforme et de politique de règlement des différends après délégation qui

accompagnent ce module. Les opérateurs de registre peuvent introduire des mesures de protection des droits supplémentaires pertinentes au gTLD spécifique.

Mettre en œuvre des mesures de protection des noms de pays et de territoires dans le nouveau gTLD. Tous les nouveaux opérateurs de registre gTLD sont tenus de fournir certaines protections minimales pour les noms de pays et de territoires, notamment en appliquant une réservation initiale, ainsi que l'établissement des règles et procédures applicables concernant la publication de ces noms. Les opérateurs de registre sont invités à mettre en œuvre des mesures de protection des noms géographiques en plus de celles rendues obligatoires par le contrat, selon les besoins et les intérêts en jeu en fonction des circonstances propres à chaque gTLD. (Voir la Spécification 5 de la version préliminaire du contrat de registre).

Payer les frais récurrents à l'ICANN. En plus des dépenses existantes réalisées pour remplir les objectifs définis dans la déclaration de mission de l'ICANN, ces fonds permettent d'apporter le soutien nécessaire aux nouveaux gTLD, notamment en ce qui concerne : la conformité contractuelle, la liaison des registres, l'augmentation des accréditations des bureaux d'enregistrement et d'autres activités de soutien au registre. Les frais incluent un composant fixe (25 000 dollars US par an) et, lorsque le TLD dépasse une certaine taille, des frais variables basés sur le volume de transaction. Voir l'article 6 de la version préliminaire du contrat de registre.

Remettre régulièrement un dépôt de données. Cela joue un rôle important dans la protection du requérant et dans la continuité de certaines instances, au cours desquelles le registre ou un aspect de son fonctionnement subit un échec du système ou une perte de données. (Voir la Spécification 2 de la version préliminaire du contrat de registre.)

Fournir des rapports mensuels de façon ponctuelle. Un opérateur de registre doit fournir un rapport à l'ICANN chaque mois. Ce rapport doit comporter les statistiques de performance pour le mois en cours, les transactions du registraire, ainsi que d'autres données. Il est utilisé par l'ICANN pour des raisons de conformité ainsi que pour le calcul des frais de requérant. (Voir la Spécification 3 de la version préliminaire du contrat de registre.)

Fournir le service Whois. Chaque opérateur de registre doit fournir un service Whois disponible publiquement pour les noms de domaines enregistrés dans le TLD. (Voir la Spécification 4 de la version préliminaire du contrat de registre.)

Entretenir des partenariats avec les bureaux d'enregistrement accrédités par l'ICANN. Chaque opérateur de registre crée un accord registre-registraire (RRA) pour définir les exigences à l'égard de ses registraires. Cet accord doit comporter certains termes qui sont spécifiés dans le contrat de registre. Il peut par ailleurs inclure des conditions supplémentaires spécifiques au TLD. L'opérateur de registre doit fournir un accès non discriminatoire à ses services de registre pour tous les bureaux d'enregistrement accrédités par l'ICANN avec lesquels il a conclu un accord RRA et qui sont en conformité avec les exigences définies. Cela implique la notification anticipée des modifications tarifaires à l'ensemble des bureaux d'enregistrement en conformité avec les délais prévus dans l'accord. (Voir l'article 2 de la version préliminaire du contrat de registre.)

Proposer un point de contact pour le signalement des abus. L'opérateur de registre doit proposer et publier sur son site Internet un point de contact unique responsable du traitement des problèmes nécessitant une attention immédiate, et en charge de répondre rapidement aux plaintes signalant un abus pour tous les noms enregistrés dans le TLD par l'intermédiaire de tous les bureaux d'enregistrement, notamment ceux impliquant un revendeur. (Voir la Spécification 6 de la version préliminaire du contrat de registre.)

Coopérer dans le cadre des audits de conformité contractuelle. Pour préserver l'équité et proposer un environnement de fonctionnement cohérent, le personnel de l'ICANN effectue des audits périodiques afin d'évaluer la conformité contractuelle et de résoudre les éventuels problèmes soulevés. L'opérateur de registre doit fournir les documents et les informations demandés par l'ICANN. Ils sont nécessaires pour réaliser de tels audits. (Voir l'article 2 de la version préliminaire du contrat de registre.)

Maintenir un instrument assurant la continuité des opérations. L'opérateur de registre doit, tout au long de la validité du contrat, mettre à disposition un instrument assurant la continuité des opérations qui sera suffisant pour

financer les opérations de registre de base pendant une période de trois (3) ans. Cette obligation reste valable pendant les cinq (5) ans suivant la délégation du TLD. À l'issue de cette période, l'opérateur de registre n'est plus tenu de maintenir l'instrument assurant la continuité des opérations. (Voir la Spécification 8 de la version préliminaire du contrat de registre.)

Soutenir les politiques et procédures communautaires. Si l'opérateur de registre a donné à son application un statut communautaire, son contrat de registre l'oblige à soutenir les politiques et les procédures communautaires spécifiés dans son application. L'opérateur de registre est soumis à la procédure de règlement des différends concernant les restrictions des registres en ce qui concerne les litiges relatifs à l'exécution des politiques et procédures communautaires. (Voir l'article 2 de la version préliminaire du contrat de registre.)

Disposer de plans de continuité et de transition en place. Cela inclut la désignation d'un fournisseur de transition, ainsi que la réalisation d'un test régulier de bascule. Au cas où une transition vers un nouvel opérateur de registre devient nécessaire, celui-ci doit coopérer en consultant l'ICANN au sujet du successeur approprié, en fournissant les données requises en vue d'une transition en douceur et en respectant les procédures de transition de registre applicables. (Pour consulter une discussion relative aux procédures de transition, voir la note explicative « Processus de transition de registre ».)

Assurer la disponibilité de fichiers de zone TLD via un processus standardisé. Cela comprend la fourniture d'un accès au fichier de zone du registre aux utilisateurs identifiés, d'après les normes d'accès, de fichier et de format établies. L'opérateur de registre conclut alors une forme d'accord standardisée avec des utilisateurs de fichier de zone et accepte les informations d'identification d'utilisateurs via une chambre de compensation. Pour plus d'informations, voir la Spécification 4 de la version préliminaire du contrat de registre et la proposition de stratégie « Accès au fichier de zone pour le futur ».

Implémenter les technologies DNSSEC. L'opérateur de registre doit signer les fichiers de zone TLD qui implémentent les technologies DNSSEC (Domain Name System Security Extensions) en conformité avec les normes techniques pertinentes. Le registre doit accepter le

matériel de clé publique des requérants pour les noms de domaine enregistrés dans le TLD, puis publier une déclaration de politique DNSSEC décrivant le stockage principal du matériel, l'accès aux clés de registre et leur utilisation, ainsi que le matériel d'autorité de certification des requérants. Pour plus d'informations, reportez-vous à la Spécification 6 de la version préliminaire du contrat de registre.

5.4.2 Obligations de l'ICANN

L'ICANN continuera de fournir une assistance aux opérateurs de registre de gTLD lors du lancement et de la gestion des opérations de registre. La fonction de liaison des registres de gTLD de l'ICANN offre aux opérateurs de registre de gTLD un rôle de contact pour une assistance continue.

La fonction de respect des contrats de l'ICANN effectuera également des audits réguliers pour s'assurer que les opérateurs de registre gTLD se conforment bien aux obligations du contrat, et traitent l'ensemble des plaintes émises par la communauté à propos du respect des obligations contractuelles de la part de l'opérateur de registre. Pour plus d'informations sur les activités de conformité contractuelle actuelles, voir http://www.icann.org/en/compliance/.

Les statuts de l'ICANN exigent qu'il agisse de manière ouverte et transparente, et qu'il traite équitablement l'ensemble des opérateurs de registre. L'ICANN est responsable du maintien de la sécurité et de la stabilité sur le réseau Internet mondial. Dans le cadre de cet objectif, l'ICANN cherche à bâtir une relation constructive et coopérative avec les futurs opérateurs de registre gTLD.