INSTANTANÉ DU PROGRAMME PRÉLIMINAIRE DE DÉVELOPPEMENT[1]

DOMAINES DE PREMIER NIVEAU DE HAUTE SÉCURITÉ (TLD)

GROUPE CONSULTATIF

[1] Instantané du développement pris du wiki du groupe de travail sur la HSTLD et de liste de diffusion du 17-2-2010

STATUT DE CE DOCUMENT

Ce document est un instantané du développement des activités en cours ou réalisées par le groupe consultatif sur les TLD de zone de haute sécurité des TLD (« GC HSTLD »). Le travail préliminaire présenté dans ce document reflète les efforts continus de développement autour d'un programme volontaire conçu pour soutenir les normes de contrôle et les stimulations visant à renforcer la confiance dans les TLD qui choisissent de participer au programme.

SOMMAIRE

Nous soumettons ce rapport à la communauté de l'ICANN pour solliciter des commentaires dans le cadre du travail en cours sur l'élaboration du guide de candidature pour les nouveaux noms de domaine génériques de premier niveau (gTLD). Le travail reflété dans ce rapport est considéré comme un « travail en évolution », au fur et à mesure que nous développons un programme volontaire d'extensions de haute sécurité.

NORMES DU DOCUMENT

En tant qu'instantané du développement, le contenu de ce document est une combinaison de brèves descriptions et de l'état actuel des éléments du programme actuellement en cours de développement dans le cadre du programme HSTLD. Pour permettre la distinction entre les descriptions des éléments du programme et le contenu du développement du programme à proprement parler, les descriptions des éléments du programme sont en écriture de texte normale et le contenu du développement du programme en italique.

Table des matières

1.0 SYNTHÈSE

Travail initial sur un programme volontaire consistant en normes de contrôle et stimulations visant à renforcer la confiance dans les TLD qui choisissent de participer au programme, produit avant la conférence internationale de l'ICANN à Séoul. Au cours de la période de temps conduisant à la conférence de Séoul, le personnel de l'ICANN a produit une note conceptuelle décrivant dans leurs grandes lignes les réflexions initiales sur la façon selon laquelle un programme volontaire pourrait être réalisé. La note conceptuelle a été publiée en tant que composante de la 3ème version préliminaire du guide de candidature aux nouveaux gTLD et peut être visualisée sur le lien suivant :

http://www.icann.org/en/topics/new-gtlds/high-security-zone-verification-04oct09-en.pdf

La réponse de la communauté à la note conceptuelle était en grande partie positive. Pour poursuivre le soutien au développement du concept, l'ICANN a invité des membres de la communauté à participer à un groupe consultatif sur la HSTLD (« GC HSTLD »). Le GC HSTLD se compose actuellement de membres du personnel de l'ICANN et de membres de la communauté qui ont exprimé un intérêt à aider à l'élaboration du programme ainsi que de particuliers experts dans des disciplines liées au programme (par ex. sécurité, vérification, programmes de certification). Le GC HSTLD se réunit régulièrement pour, se basant sur les concepts introduits dans le document initial, rédiger des éléments de contrôle et des exigences du programme, et publier un programme décisionnel à proposer à la considération et à la révision de la communauté. Ce document présente les sujets les plus récents en cours de révision ou d'élaboration par le GC HSTLD.

Le GC HSTLD mène ses activités et le développement du programme selon un processus ouvert et transparent. Cet instantané du développement est une composante de ce processus. Des informations supplémentaires y compris les noms des membres du groupe et les enregistrements des réunions hebdomadaires du GC HSTLD sont disponibles à partir du lien suivant :

http://www.icann.org/en/topics/new-gtlds/hstld-program-en.htm

2.0 ACTIVITÉS DE DÉVELOPPEMENT

Les activités de développement les plus importantes effectuées depuis la conférence internationale de l'ICANN à Séoul en Corée comprennent :

- Établissement du GC HSTLD et révision de la note conceptuelle initiale par le GC HSTLD ;
- Documentation des exigences premières et de la logique de la HSTLD ;
- Travail supplémentaire afin d'améliorer le contenu de la note conceptuelle initiale y compris les composantes de ses fondements :
  - Déclaration d'objectif du groupe
  - Déclaration des problèmes de la HSTLD
  - Déclaration des bénéfices de la HSTLD ;
- Travail supplémentaire afin d'améliorer les principes, thèmes, objectifs, critères d'échantillonnage ; et
- Ajout d'un nouveau concept de « carnet de correspondance ».

Le reste de cet instantané du développement expliquera chacune des activités ci-dessus et présentera leur état actuel de développement en tant qu' « instantané » dans le temps. Le GC HSTLD utilise ses réunions hebdomadaires, sa messagerie, un wiki du GC HSTLD et d'autres outils de collaboration afin de développer la documentation du programme HSTLD. En fin de compte, la documentation produite par le GC HSTLD sera utilisée afin de créer les éléments clé d'un programme HSTLD décisionnel. Le GC publiera alors le programme pour une sollicitation de commentaires du public.

2.1 Établissement du GC HSTLD

Le travail a commencé sur l'amélioration d'un concept de programme HSTLD volontaire à travers le parrainage de la part de l'ICANN d'un groupe consultatif composé de membres du personnel de l'ICANN et de membres intéressés de la communauté. Le groupe a été établi pour continuer à développer la documentation du concept HSTLD volontaire initialement publiée en tant que composante de la conférence internationale de l'ICANN à Séoul en Corée. La première réunion du GC HSTLD a eu lieu le 6 janvier 2010 et le groupe continue à se réunir à une fréquence hebdomadaire pour travailler sur le développement du concept du programme HSTLD. L'état des efforts de développement du groupe, les actualisations des instantanés du développement et, en fin de compte, une nouvelle note conceptuelle (si le lancement du programme est envisagé) seront présentés au cours des conférences internationales de l'ICANN.

2.2 Documentation des exigences premières et de la logique de la HSTLD ;

Lors de l'établissement du GC HSTLD, le groupe a énuméré les exigences premières et la logique sous-tendant la note conceptuelle HSTLD, pour aider au développement de la documentation fondamentale. Cette documentation a été rassemblée et peut être visualisée à partir du lien suivant :

http://mm.icann.org/pipermail/hstld-ag/2010-January/000094.html

2.3 Aperçu général de la documentation du développement

Un des premiers domaines d'intérêt du GC HSTLD a été l'objectif du groupe HSTLD, les problèmes et les bénéfices. Ces domaines constituent les fondements d'un programme HSTLD bien exécuté, et servent en tant que lignes directrices globales sur lesquelles le programme HSTLD est fondé. Pour le moment, la discussion au sein du GC HSTLD a progressé au-delà de ces domaines, mais ils seront reconsidérés en tant que de besoin tout au long des efforts globaux de développement de la HSTLD.

Au cours de l'élaboration des déclarations d'objectif, de problèmes et de bénéfices, les membres du GC HSTLD ont suggéré une nouvelle méthode de comptes-rendus, à l'intention des TLD intéressés par le fait de devenir des TLD HSTLD. La nouvelle méthode de compte-rendu est fondée sur un concept de « carnet de correspondance ». Elle fournit aux TLD une méthode d'auto-certification de leur conformité au programme HSTLD. Le GC évaluera cette méthode de compte-rendu et la comparera à d'autres programmes de certification, de marque de confiance et de vérification similaires.

Suite à la création et à la discussion de la documentation de l'objectif, des problèmes et des bénéfices de la HSTLD, le GC HSTLD s'est concentré sur les principes, les thèmes, les objectifs et les critères d'échantillonnage. Ce matériel est celui qui a été le plus récemment discuté et est toujours en train d'être activement élaboré.

Chacune de ces sections sera brièvement décrite ci-dessous, le texte en écriture normale décrivant la documentation et le texte en italique représentant les documents préliminaires de travail du GC HSTLD.

2.4 Déclaration d'objectif du groupe

La première tâche du développement entrepris par le GC HSTLD fut de façonner une déclaration d'objectif du groupe GC HSTLD. La déclaration d'objectif du groupe GC HSTLD fournit à la communauté une charte de l'objectif global du GC HSTLD. Elle fournit à la communauté et aux membres du GC HSTLD une méthode de communication de l'objectif global et de l'orientation. La version préliminaire actuelle de la déclaration d'objectif du GC HSTLD est comme suit :

« L'objectif du groupe consultatif sur les domaines de premier niveau de zone de haute sécurité est de réunir les représentants de la communauté afin d'évaluer la viabilité d'un programme volontaire soutenant des normes de contrôle et des stimulations qui pourraient être potentiellement adoptées afin de fournir un niveau renforcé de confiance et de sécurité au-dessus des contrôles de base d'enregistrement-autorisation ».

2.5 Déclaration des problèmes du groupe

Alors que le GC HSTLD commençait à façonner une déclaration d'objectif appropriée, plusieurs membres du GC ont soulevé la question de définition des problèmes que le GC HSTLD était appelé à résoudre, afin que ces problèmes soient documentés et disponibles à la révision de la communauté. Cette documentation aidera le GC HSTLD à rester concentré, au fur et à mesure que des contrôles conçus pour réduire ces problèmes seront produits. La déclaration de problèmes du GC HSTLD est comme suit :

« Certains particuliers/organisations ont cherché à exploiter des vulnérabilités au sein de la technologie du DNS, et les pratiques commerciales de certaines autorités d'enregistrement, à des fins inappropriées et/ou illégales. L'exploitation de ces vulnérabilités a menacé la sécurité et la stabilité de l'Internet et a eu un impact négatif sur la confiance des utilisateurs lors de l'utilisation de l'Internet.

Plusieurs sont les parties intéressées :

1. *Les titulaires de noms de domaine souhaiteraient s'assurer que le nom qu'ils enregistrent ne sera pas piraté suite à la compromission du compte du bureau d'enregistrement/du registre ou de leur propre compte. (y compris le DNS, le WHOIS, etc)*
2. *Les bureaux d'enregistrement souhaiteraient pouvoir donner aux titulaires de noms de domaine des garanties raisonnables que le cas n.1 n'aura pas lieu parce qu'ils disposent de contrôles. Afin de le faire, ils ont besoin de la coopération autant des titulaires de noms de domaine que des registres.*
3. *Les registres souhaiteraient également obtenir l'assurance exprimée au n.1 et ceci exige la coopération du titulaire de nom de domaine et du bureau d'enregistrement.*
4. *Les utilisateurs finaux souhaiteraient savoir que lorsqu'ils saisissent un nom de domaine donné, ou lorsqu'ils naviguent à partir d'un signet, etc., ils se dirigent vers le bon domaine, et que le DNS, etc., n'a pas été piraté.*
5. *Les utilisateurs finaux souhaiteraient comprendre qu'un nom de domaine enregistré dans un gTLD particulier est sujet à des normes d'enregistrement, des politiques et des procédures visant à réduire la conduite malveillante de tels titulaires de noms de domaine ».*

2.6 Déclaration de bénéfices du groupe

A ce jour, le dernier domaine de fondement du développement du programme est l'élaboration d'une déclaration de bénéfices de la part du GC HSTLD. Le but ultime de la documentation des bénéfices est d'aider la communauté à comprendre quels bénéfices pourraient être réalisés de par l'adhésion à un programme HSTLD. Cette documentation n'est pas destinée à être une analyse détaillée de valeur et de bénéfices. Elle est plutôt destinée à présenter les bénéfices globaux pour la communauté, déclinés par les groupes les plus concernés par le programme HSTLD. La documentation actuelle du GC HSTLD relative aux bénéfices est comme suit :

« Les registres profitent :

Ry1. en démontrant qu'ils suivent des normes rigoureuses régissant la continuité, la sécurité et l'intégrité opérationnelle à travers un processus d'audit

Ry2. en démontrant qu'ils ont des activités commerciales qui ont été révisées et trouvées conformes aux normes d'intégrité organisationnelle, opérationnelle et financière

Ry3. en démontrant qu'ils disposent de traitement de données, de stockage et de méthodes qui satisfont les normes rigoureuses de confidentialité, précision, intégrité, récupération des données, etc.

Ry4. en démontrant qu'ils ont mis en œuvre des pratiques et des mesures visant à minimiser les abus des services de noms de domaine et d'enregistrement de noms de domaine

Ry5. en satisfaisant les points (Ry1) à (Ry4), ce qui donne confiance aux utilisateurs finaux et aux titulaires de noms de domaine concernant la solidité financière et la fiabilité de leurs entreprises,

et garantit que les mesures visant à réduire la fréquence d'enregistrement de domaines malveillants sont appliquées par les bureaux d'enregistrement qui traitent les enregistrements pour le registre

Les bureaux d'enregistrement profitent :

Rr1. en démontrant qu'ils satisfont toutes les normes régissant la continuité, la sécurité et l'intégrité opérationnelle « diffusées par percolation » par un registre HSTLD à travers un processus d'audit. (« trickle down » signifie que le bureau d'enregistrement applique toute condition imposée au registre qui ne peut être satisfaite sans l'assistance du bureau d'enregistrement, par ex. une condition qui a un impact sur l'interface bureau d'enregistrement-titulaire de nom de domaine)

Rr2. en démontrant que leurs activités commerciales ont été révisées et trouvées conformes aux normes d'intégrité organisationnelle, opérationnelle et financière « diffusées par percolation » par un registre HSTLD

Rr3. par « percolation » du Ry3

Rr4. par « percolation » du Ry4

Rr5. en satisfaisant les points (Ry1) à (Ry4), ce qui donne confiance aux utilisateurs et aux titulaires de noms de domaine concernant le fait que la HSTLD a confiance en le bureau d'enregistrement pour traiter les enregistrements pour le compte du registre. Les normes les plus rigoureuses régissant le traitement de l'enregistrement garantissent également aux utilisateurs et titulaires de noms de domaine que les données d'enregistrement sont précises, que les plaintes pour abus sont traitées selon les pratiques standards, etc.

Les titulaires de noms de domaine profitent :

Re1. en démontrant qu'ils sont disposés à se soumettre à des mesures de vérification rigoureuses associées à un registre HSTLD

Re2. en démontrant qu'ils sont disposés à maintenir des données d'enregistrement exactes (et à se conformer aux mesures de vérification mises en œuvre pour s'assurer que les données sont exactes)

Re3. en démontrant qu'ils sont disposés à accepter les modalités de services et procédures convenues qui énumèrent les usages interdits et les abus et habilitent les registres/bureaux d'enregistrement à suspendre ou à réagir autrement pour faire face aux violations de modalités de service ou de procédures convenues

Re4. des mesures mises en œuvre afin de minimiser les enregistrements de domaines malveillants : un grand nombre de ces mesures rend la compromission d'un compte de titulaire de nom de domaine légitime plus difficile aux attaquants

Re5. des mesures mises en œuvre afin de minimiser l'abus du DNS : un grand nombre de ces mesures rend la compromission d'un compte de titulaire de nom de domaine légitime et l'altération des données de configuration du DNS plus difficiles aux attaquants.

Les utilisateurs profitent :

U1. de données d'enregistrement plus exactes

U2. d'incidents d'enregistrements malveillants et d'abus de DNS moins fréquents parmi les noms de domaine enregistrés dans un HSTLD

U3. de processus de traitement des abus clairement définis »

2.7 Concept de « carnet de correspondance »

Alors que le GC HSTLD élaborait le matériel de fondement ci-dessus, des questions ont été soulevées concernant le processus de certification de la note conceptuelle initiale de vérification. La note conceptuelle initiale utilisait une méthode de vérification de tiers en tant que mécanisme de communication de l'adoption des contrôles du programme HSTLD par un TLD à l'ensemble de la communauté. A travers la discussion de groupe, une méthode alternative (bien que non incompatible) de communication de l'adoption des contrôles HSTLD par un TLD a été présentée. La méthode alternative est fondée sur le concept de carnet de correspondance que les TLD peuvent remplir pour communiquer à la communauté leur conformité aux contrôles HSTLD. Un aperçu très général du concept suit :

« Carte de pointage sécurité de TLD

L'ICANN ne fournit pas actuellement de critères de mesure permettant aux titulaires de noms de domaine de prendre une décision avisée concernant les options d'enregistrement de leurs noms de domaine. La carte de pointage sécurité serait un concept qui pourrait être intégré aux accessoires actuels du tableau de bord de l'ICANN.

Cette carte de pointage comprendrait une matrice des critères de contrôle convenus sur l'axe des y et « tous » les opérateurs de registres TLD sur l'axe des x. Chaque case de la matrice serait conforme au schéma de couleurs suivant :

- *Case blanche/vide : L'opérateur de registre n'a pas fourni de données à propos de cet élément de contrôle.*
- *Case hachurée jaune : L'opérateur de registre a « auto-certifié » sa conformité à cet élément de contrôle.*
- *Case hachurée vert à 50% : Un tiers à vérifié la conformité du registre à cet élément de contrôle à un moment spécifique dans le temps, mais n'a pas pu établir une conformité à long terme.*
- *Case hachurée vert à 100% : Un tiers a vérifié la conformité du registre à cet élément de contrôle sur une période de conformité à long terme.*
- *Case hachurée rouge : Dans le cas où un registre « a auto-certifié » un critère de contrôle spécifique mais qu'il a été constaté qu'il n'était pas conforme. Il est envisagé que toutes fausses déclarations concernant l'auto-certification serait une violation de l'accord de registre et ferait l'objet d'une enquête de la part du personnel de l'ICANN chargé de la conformité ».*

2.8 Principes, thèmes, objectifs, critères d'échantillonnage

La section 3.2.1 de la note conceptuelle initiale comprenant des détails sur les exigences essentielles du programme HSTLD. Cette section représente une collection de principes, objectifs et critères qui forment la base des contrôles réels conçus pour améliorer la sécurité et la confiance des TLD. Le GC HSTLD travaille en vue d'améliorer cette section. Très récemment, les principes initiaux ont été révisés et un principe préliminaire supplémentaire (actuellement énuméré « Principe 4 ») est en cours de discussion avant d'être finalement ajouté aux principes. Le GC HSTLD est actuellement en train

d'évaluer les « thèmes de critères possibles », dans un effort pour se mettre d'accord sur des critères réels et des exemples de contrôle illustratifs. Lorsqu'ils seront complétés, chaque thème de critère sera associé à un ou plus d'exemples de contrôle illustratifs à titre de conseils en matière de contrôles appropriés nécessaires pour satisfaire les exigences des critères. L'instantané du développement actuel de cette section est comme suit :

« PRINCIPE 1 : Le registre maintient des dispositifs de contrôle efficaces pour raisonnablement garantir que la sécurité, la disponibilité et la confidentialité des systèmes et des éléments d'actif informationnel soutenant les TI décisives du registre (soit les services d'enregistrement, les bases de données du registre, l'administration des zones et la prestation de services de résolution de noms de domaine) et les opérations d'affaires sont maintenues de par l'exécution de ce qui suit :

- *définition et communication des objectifs de performance, des politiques et des normes pour la sécurité du système et des éléments d'actif informationnel, leur disponibilité, confidentialité et droit au domaine privé ;*
- *utilisation de procédures, ressources humaines, logiciels, données et infrastructure afin de réaliser des objectifs définis conformément à des politiques et à des normes établies ; et*
- *surveillance du système et des éléments d'actif informationnel et prise de mesures afin de satisfaire la conformité aux objectifs, politiques et normes définis.*

No.	*Thème*	*Objectif*	*Thèmes de critères possibles*	*Critères*	*Contrôles illustratifs*
1.1	*Sécurité infrastructure TI du registre*	*Les éléments clés des composantes TI qui soutiennent l'infrastructure des TLD sont sécurisés et adéquatement protégés contre l'accès physique et logique non autorisé.*	*· Gestion de la sécurité* *· Sécurité du personnel* *· Contrôle de l'accès physique* *· Stockage et élimination des médias* *· Contrôles d'acquisition et de développement du système* *· Contrôles de gestion des incidents de sécurité* *· Notification et réponse aux incidents de sécurité* *· Contrôles des interfaces* *· Gestion de l'accès au système* *· Sécurité des réseaux* *· Sécurité des applications* *· Exigences de chiffrement* *· Test périodique de vulnérabilité et exercices de réponse* *· Processus de parutions du système* *· Contrôles de gestion du service de résolution des noms (par ex. surveillance de l'intégrité de la zone DNS et de la disponibilité des serveurs de noms, …)* *· Plan de déploiement des DNSSEC* *· Voies de transmission sécurisées*		

			(connexions avec les bureaux d'enregistrement authentifiées, cryptées) *· Gestion des éléments d'actif informationnel (exactitude de la base de données/intégrité/disponibilité des services pour la zone, l'enregistrement et les autres données des clients)*		
1.2	*Disponibilité infrastructure TI du registre*	*Les services TLD sont disponibles à l'usage en vertu d'un contrat ou d'un engagement*	*· Accords de niveau de services* *· Disponibilité des services Whois* *· Niveau de performance des services Whois* *· Temps de réponse des services Whois* *· Exactitude et état complet du Whois* *· Surveillance de disponibilité* *· Sauvegarde des données de transaction et d'enregistrement y compris calendrier de sauvegarde, spécifications, transfert, et vérification de sécurité* *· Plan de reprise sur sinistre et de continuité des affaires (pratiques de basculement, y compris les plans pour soutenir le service de résolution des noms en cas de défaillance d'entreprise) et exercices* *· Contrôles environnementaux (énergie et climatisation, protection contre l'incendie, générateurs)* *· Contrôles de sécurité du câblage*		
1.3	*Confidentialité et droit au domaine privé des données sensibles*	*Les données possédées, gérées ou transférées à travers les TLD désignées comme confidentielles sont protégées tel que promis ou convenu. Les données personnelles recueillies par l'opérateur du TLD sont rassemblées, utilisées, conservées, divulguées et détruites de manière appropriée, en ligne avec les lois de protection des*	*· Classification appropriée des données confidentielles et personnellement identifiables* *· Politiques de rassemblement, d'utilisation, de conservation, d'accès et de divulgation des données* *· Données au repos et en transit* *· Accès de tiers aux informations* *· Exigences de chiffrement* *· Contrôles de gestion pour les clés de signature* *· Contrôles de l'accès physique et*		

		données pertinentes selon la juridiction de l'opérateur du registre.	*logiques* *· Séparation des fonctions* *· Surveillance du système* *· Contrôles de sécurité personnelle*		

PRINCIPE 2 : Le registre maintient des dispositifs de contrôle efficaces pour raisonnablement garantir que le traitement des fonctions essentielles du registre est autorisé, exact, complet et exécuté de manière opportune conformément à des politiques et normes établies. L'identité des entités participantes est établie et authentifiée.

No.	*Thème*	*Objectif*	*Thèmes de critères possibles*	*Critères*	*Contrôles illustratifs*
2.1	*Vérification de sécurité du registre*	*Les qualifications de l'opérateur du registre sont mises à disposition pour prouver l'identité de l'entité légale qui dirige le TLD.*	*· Validation de l'organisation du REGISTRE, y compris* *- Antécédents des directeurs* *- Adresse vérifiable* *- Adresse électronique vérifiable* *- Numéros de téléphone vérifiables* *- Statuts* *- Certificat de constitution* *- Documents de charte* *- Licence professionnelle* *- Faisant des affaires en tant que (soit nom d'emprunt)* *- Enregistrement de l'appellation commerciale* *- Documents de partenariat* *- Licence professionnelle* *· Couverture d'assurance* *· Capacités financières* *· Exigences de revalidation* *· Processus de sélection des employés*		
2.2	*Vérification de sécurité du bureau d'enregistrement*	*L'identité du bureau d'enregistrement est désignée et établie avant le démarrage des opérations*	*· Validation de l'organisation du BUREAU D'ENREGISTREMENT, thèmes notés au 2.1* *· État d'accréditation du bureau d'enregistrement* *· Exigences de revalidation*		
2.3	*Intégrité de traitement du registre*	*Les données du TLD sont cohérentes et correctes au niveau du registre du TLD.*	*· Maintenance et enregistrement du nom de domaine* *· Maintenance, exactitude, état complet et intégrité des données publiques Whois* *· Validation du nouveau bureau*		

			d'enregistrement *· Processus de surveillance continus* *· Révison qualité/AQ des données du bureau d'enregistrement (et résultats de l'audit de sauvegarde des données)* *· Processus de règlement des différends*		
2.4	*Politique anti-abus et application*	*Établir des dispositifs de contrôle efficaces afin de réduire la conduite malveillante de la part des bureaux d'enregistrement et des titulaires de noms de domaine*	*· Contrôles anti-hameçonnage et anti-mystification pour les nouveaux TLD* *· Notation(s) par des tiers indépendants appartenant à des analystes et laboratoires réputés en anti-hameçonnage et anti-logiciels malveillants* *· Accords sur les niveaux de service basés sur un pourcentage de domaines malveillants par « unité de mesure » d'enregistrement (par ex. 1 000, 5 000, 10000 domaines)* *· Politique de serveurs de noms orphelins (déclaration des actions qui seront entreprises pour identifier et corriger les serveurs de noms orphelins)* *· Points de contact en cas d'abus et processus de réponse documenté, opportun et vérifiable* *· Définition de l'utilisation malveillante (conduite), interdiction explicite de toute conduite malveillante dans l'accord de modalités de service du titulaire de nom de domaine* *· Processus de suspension de domaine rapide* *· Processus et soutien Whois épais* *· Plan de déploiement des DNSSEC & IPv6* *· Surveillance de zone en temps réel (par ex. pour surveiller les activités suspectes, par ex. le fast flux)* *· Rapports mensuels des activités malveillantes notifiées au registre (telles que hameçonnage et réseaux de zombies) et engagement en*		

			matière de prise de mesures si les résultats sont importants (par rapport à d'autres bureaux d'enregistrement qui font des affaires avec ce registre)		

PRINCIPE 3 : Le registre maintiendra des dispositifs de contrôle efficaces pour raisonnablement garantir que le traitement des fonctions essentielles du registre par ses bureaux d'enregistrement est autorisé, exact, complet et exécuté de manière opportune conformément à des politiques et normes établies. L'identité des entités participantes est établie et authentifiée.

No.	*Thème*	*Objectif*	*Thèmes de critères possibles*	*Critères*	*Contrôles illustratifs*
3.1	*Vérification de sécurité du titulaire du nom de domaine*	*L'identité du titulaire du nom de domaine est vérifiée et établie avant que le bureau d'enregistrement ne mette le nom de domaine à sa disposition.*	*· Thèmes de validation de l'organisation notés au 2.1* *· Autorité du titulaire du nom de domaine à s'enregistrer dans le TLD* *· Utilisateurs commerciaux exempts d'intermédiation/enregistrements (le candidat doit fournir des preuves qu'il s'agit d'une personne physique, une organisation doit démontrer la raison ou la justification de l'anonymat)*		
3.2	*Intégrité de traitement du bureau d'enregistrement*	*Les données sont cohérentes et correctes au niveau du bureau d'enregistrement.*	*· Authentification des nouveaux titulaires de noms de domaine par le bureau d'enregistrement selon des processus convenus* *· Confirmation par le bureau d'enregistrement que les données d'enregistrement sont exactes et complètes* *· Surveillance des données d'enregistrement par le bureau d'enregistrement pour vérifier leur exactitude et état complet* *· Authentification par le bureau d'enregistrement des données d'enregistrement pour chaque transaction* *· Confirmation par le bureau d'enregistrement de changements des données d'enregistrement* *· Rejet/suspension de données d'enregistrement s'il y a lieu (incomplètes, fausses/inexactes)* *· Whois épais*		

			· Élimination de données d'enregistrement par le bureau d'enregistrement *· Processus de surveillance continus* *· Révision AQ périodique des données des titulaires de noms de domaine* *· Processus de démontage et objectifs de ponctualité (par ex. délai moyen de réparation)*		

PRINCIPE 4 : Les titulaires de noms de domaine dans une zone de haute sécurité sont censés maintenir des données exactes et actuelles et s'engager à s'abstenir de toutes activités conçues pour troubler ou tromper le public internaute.

No.	*Thème*	*Objectif*	*Thèmes de critères possibles*	*Critères*	*Contrôles illustratifs*
4.1	*Exactitude des données des titulaires de noms de domaine*	*Les titulaires de noms de domaine fournissent des données d'identité et locatives exactes et actuelles*	*Données WHOIS* *Données locatives du titulaire de nom de domaine fournies au registre* *Données de contact fournies au registre* *Absence d'intermédiaires*		
4.2	*Conduite du titulaire du nom de domaine*	*Les titulaires de noms de domaine s'engagent explicitement à respecter les politiques de l'ICANN, ainsi que toutes obligations supplémentaires créées de par l'application des normes HSTLD*	*Code de conduite »*		

3.0 Prochaines étapes

Le GC HSTLD continuera à développer la documentation dans le cadre de ses efforts visant à améliorer la note conceptuelle HSTLD initiale. Les prochaines étapes immédiates comprennent sans y être limitées la poursuite des réunions hebdomadaires du groupe, la réunion à Nairobi, et le développement continu de la documentation clé du programme y compris :

- La documentation de fondement ;
- Le concept du « carnet de correspondance » versus d'autres options alternatives ;
- Les principes, objectifs, critères et exemples illustratifs ; et
- La gouvernance globale du programme et les acteurs.

Tel que mentionné précédemment, les instantanés et du développement et les actualisations de la note conceptuelle initiale seront publiés lors des conférences internationales de l'ICANN.