Rapport initial du groupe de travail d'experts sur un service d'annuaire d'enregistrement de nouvelle génération

STATUT DU PRÉSENT DOCUMENT

Voici un rapport du groupe de travail d'experts (EWG) qui donne des recommandations pour un service d'annuaire d'enregistrement gTLD de nouvelle génération (« RDS ») pour remplacer le système WHOIS actuel.

I. RÉSUMÉ 3
II. MANDAT ET OBJECTIFS DE L'EWG 9
2.1 Mandat 9
2.2 Déclaration d'intention pour guider le travail de l'EWG 10
III. MÉTHODOLOGIE - IDENTIFIER LES UTILISATEURS ET LES OBJECTIFS 11
3.1 Méthodologie du cas d'utilisation 11
3.2 Identifier les utilisateurs du RDS 13
3.3 Identifier les objectifs à adopter ou à interdire 17
3.4 Parties prenantes impliquées dans le RDS 19
3.5 Identification des points communs 21
3.6 Éléments de données identiques à des fins acceptables 21
IV. FONCTIONNALITÉS SOUHAITÉES ET PRINCIPES DE CONCEPTION 23
V. MODÈLE SUGGÉRÉ 32
5.1 Examen de plusieurs modèles de système 33
5.2 Proposition d'un RDS intégré 35
VI. RÉPONDRE À DES INQUIÉTUDES EN MATIÈRE DE CONFIDENTIALITÉ 38
VII. IILLUSTRATION DES FONCTIONNALITÉS D'ACCÈS SÉCURISÉ 39
VIII. CONCLUSION ET PROCHAINES ÉTAPAES 41

I. RÉSUMÉ

Le groupe de travail d'experts du service d'annuaire d'enregistrement des gTLD (EWG) a été formé par le Président-directeur général de l'ICANN, Fadi Chehadé, à partir d'une demande du Conseil d'administration dans le but d'aider à résoudre au sein de la communauté de l'ICANN l'impasse de presque dix ans sur la manière de remplacer le système WHOIS actuel, qui est largement considéré comme « cassé ». Le mandat du groupe de travail est de réexaminer et de définir l'objectif de la collecte et du maintien des services d'annuaire des gTLD, de considérer comment sauvegarder les données, et de proposer une solution de nouvelle génération pouvant mieux servir aux besoins de la communauté Internet mondiale. Le groupe a démarré son travail de zéro. Il a analysé et mis en question les hypothèses fondamentales sur les objectifs, utilisations, collecte, maintien et provision des données d'enregistrement ainsi que sur l'exactitude, l'accès et les besoins de privacité, et les parties prenantes concernées par les services d'annuaire des gTLD. Après avoir travaillé sur une énorme gamme de cas, et de la myriade de questions ayant été soulevées, l'EWG a conclu que le modèle actuel du WHOIS - qui donne à tous les utilisateurs le même accès public anonyme aux données d'enregistrement des gTLD (trop souvent inexactes) - devrait être abandonné. Au lieu du Whois, l'EWG recommande un changement de paradigme selon lequel les données d'enregistrement sont collectées, validées et divulguées seulement à des fins admissibles, avec certains éléments de données accessibles seulement aux demandeurs authentifiés qui sont tenus responsables de l'usage approprié.

L'EWG recommande d'inclure dans les « fins autorisées »ce qui suit :

- Contrôle du nom de domaine
- Recherche de noms de domaines
- Protection des données personnelles
- Actions légales
- Résolution des problèmes
- Exécution des contrats/réglementaire
- Achat/vente des noms de domaine
- Utilisation individuelle d'Internet
- Réduction des abus
- Provision de services Internet

techniques

L'EWG a considéré l'ensemble des parties prenantes concernées dans la collecte, enregistrement, divulgation et utilisation des données d'enregistrement des gTLD, appliquées aux objectifs associés Par la suite, des domaines de besoins communs ont été identifiés et pris en considération et l'EWG a développé des principes et des caractéristiques pour aider à concevoir un service de données d'enregistrement de nouvelle génération (RDS).
Ceci a conduit l'EWG à considérer plusieurs conceptions du système et il est arrivé à un accord sur un nouveau modèle de service de données d'enregistrement pour collecter, utiliser et divulguer les éléments de données exacts et individuels destinés à plusieurs objectifs. Chaque acteur de l'écosystème RDS a différents besoins quant aux données, différents risques, et potentiellement différentes responsabilités. Historiquement, la plupart de ces responsabilités étaient transférées aux bureaux d'enregistrement, dont l'objectif principal était de fournir des noms de domaine opérationnels aux clients payants. Vu la complexité de plus en plus grande de l'écosystème d'Internet, et à partir de l'introduction de centaines de nouveaux gTLD, il semblerait que les nouveaux acteurs devront prendre en charge certaines responsabilités découlant du fait de satisfaire un si large éventail d'objectifs des enregistrements.

La figure suivante illustre le modèle recommandé par l'EWG pour le RDS de nouvelle génération pouvant incorporer potentiellement un grand nombre de principes discutés dans ce rapport. **Éléments clés du modèle RDS intégré (« Aggregated RDS »- ARDS) :**

- L'ADRS sert comme référentiel intnégré qui contient une copie ne faisant pas autorité de tous les éléments de données collectés
- Chaque registre gTLD demeure la source officielle sur les données
- Les demandeurs (utilisateurs qui souhaitent obtenir les données d'enregistrement des gTLD du système) présentent leur candidature pour les identifiants d'accès à l'ARDS.

- Les registres et les bureaux d'enregistrement sont relevés de l'obligation de fournir les accès du Port 43 ou d'autres dispositions d'accès public.
- Dans la plupart des cas, l'ARDS donne l'accès aux données d'enregistrement en cache, données qui sont copiées des registres gTLD et maintenues à travers des mises à jour périodiques.
- L'ARDS peut aussi donner l'accès aux données « vivantes » d'enregistrement obtenues en temps réel des registres gTLD, sous demande et faisant l'objet de contrôles pour prévenir l'usage excessif ou abusif de cette option.
- l'ARDS (ou tout autre tierce partie en interaction avec ADRS) sera responsable de l'exécution des services de validation
- L'ARDS est responsable d'auditer l'accès afin de minimiser l'abus et d'imposer des pénalités et d'autres ré médiations au cas où il y aurait des accès inappropriés.
- L'ADRS gère les plaintes sur l'exactitude des données
- L'ARDS gère la concession de licences pour accéder aux données

L'ICANN contracte des fournisseurs internationaux externes pour développer et exploiter l'ARDS et supervise la conformité avec les dispositions en vigueur

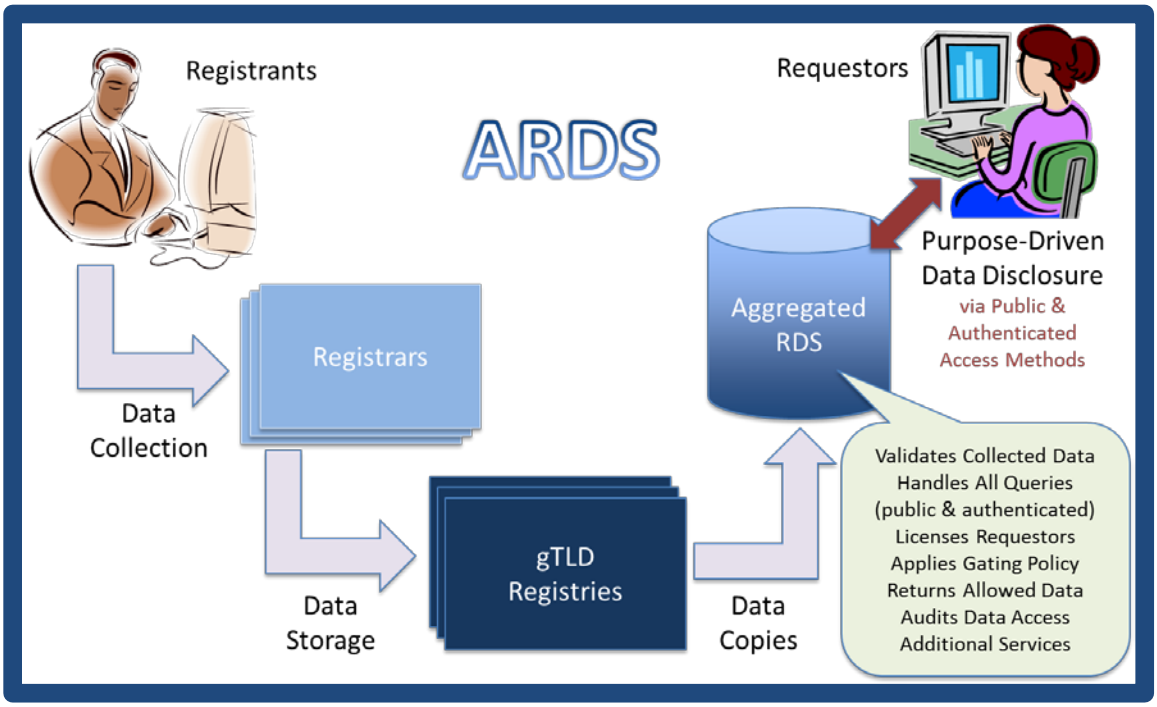

Figure 4. Modèle RDS intégré

Ce modèle a fait l'objet d'un accord de consensus de la part des membres de l'EWG en raison de ses nombreux avantages :

- Évolutivité gérée par un point de contact unique
- Améliorations potentielles du transport et de la distribution
- Système centralisé pour les demandeurs de données d'enregistrement
- Davantage de responsabilité pour la validation et l'accès aux données d'enregistrement (anti-abus)
- Capacité de suivi / audit / pénalisation des demandeurs identique à travers de multiples TLD (anti-abus)
- Réduction possible de certains coûts actuellement supportés par les registres et les bureaux d'enregistrement pour fournir des données d'accès
- La normalisation ou le filtre des données pourraient être fournis
- Réduction des exigences de bande passante pour les registres et les bureaux d'enregistrement
- Facilitation de la normalisation des approches pour répondre aux préoccupations sur la privacité des données locales
- Recherche améliorée de la capacité à travers de multiples TLD (comme la recherche inversée)
- Minimiser les coûts de transition et de mise en œuvre
- Permettre la validation / accréditation des demandeurs qui qualifient pour des objectifs spéciaux (c'est à dire, le respect de la loi)
- Faciliter la gestion plus efficace des rapports sur l'inexactitude
- Permettre des vérifications aléatoires plus efficaces en matière d'exactitude
- Permettre la visualisation d'un portail convivial pour les utilisateurs en une multiplicité de langues, scripts et caractères

Bien entendu, rien n'est parfait. L'EWG a aussi considéré les désavantages potentiels de ce modèle, à savoir :

- Latence des données
- Création d'une source « grandes données » de données informatiques de grande valeur pouvant faire l'objet d'une utilisation abusive potentielle au cas où elles ne seraient pas auditées et maintenues convenablement
- Risque accru d'abus interne et d'attaque externe, exigeant une plus grande attention dans la mise en œuvre, les normes et l'audit de la politique de sécurité

- Les registres et les bureaux d'enregistrement ne contrôlent plus la distribution des données d'enregistrement

En proposant ce nouveau modèle, l'EWG reconnaît le besoin d'exactitude ainsi que le besoin de protéger la privacité des registrants demandant des protections renforcées de leur information personnelle. L'EWG a discuté les modalités selon lesquelles le RDS serait en mesure de prendre en compte les besoins des utilisateurs vis-à-vis des risques pour une plus grande protection des services d'enregistrement en utilisant des « identificateurs protégés et sécurisés ». Une option serait l'existence d'une organisation accréditée par l'ICANN et indépendante agissant comme agent de confiance, utilisant un ensemble de critères accordés, qui déterminerait si un registrant qualifie pour une protection maximale. L'EWG espère pouvoir analyser des modèles potentiels d'identificateurs protégés et sécurisés innovants, capables de fournir un équilibre efficace entre la responsabilité et les besoins de privacité des données personnelles des utilisateurs d'Internet vis-à-vis des risques.

Prochaines étapes

Nonobstant le progrès reflété dans ces recommandations, l'EWG n'a pas fini ses délibérations. Le groupe demande à la communauté de présenter ses commentaires sur ces recommandations préliminaires et continuera à peaufiner ses recommandations en même temps qu'il analyse soigneusement les commentaires reçus en ligne, lors de la réunion de l'ICANN à Durban et à travers d'autres consultations publiques.

En outre, d'autres questions clés doivent encore être profondément analysées, à savoir :

- Conversion des fichiers obligatoires/optionnels pour chaque objectif
- Identifier les domaines qui demandent une analyse du risque et de l'impact
- Considérer les coûts et les impacts et les manières de les supporter

- Examiner les méthodes d'accès multi-modal et la manière dont elles pourraient être compatibles avec les protocoles d'accès aux données d'enregistrement actuels ou futurs.

Suite à la consultation publique de ce rapport initial, l'EWG publiera et fera parvenir un rapport final au Président-directeur général de l'ICANN et au Conseil d'administration pour servir de fondement à la politique des nouveaux gTLD et aux négociations contractuelles, le cas échéant. Tel que spécifié par le Conseil d'administration, un rapport fondé sur le rapport final sera la base pour la mise en œuvre d'un processus de développement de politiques (PDP) de la GNSO fortement ciblé, initié par le Conseil d'administration

II. MANDAT ET OBJECTIFS DE L'EWG

2.1 Mandat

L'EWG a été convoqué pour exécuter, dans une première étape, la directive du Conseil d'administration de l'ICANN[1] pour redéfinir l'objectif et la fourniture des données d'enregistrement gTLD (comme le WHOIS), afin de constituer la base de création d'une nouvelle politique globale pour les services d'annuaire gTLD et les négociations contractuelles. Les objectifs de l'EWG sont : 1) définir le but de la collecte et du maintien des données d'enregistrement des gTLD et considérer la façon de sauvegarder ces données, et 2) proposer un modèle pour gérer les services d'annuaire gTLD capable de répondre aux problèmes d'exactitude et d'accès aux données, tout en prévoyant des sauvegardes destinées à protéger les données. L'EWG a été informé par le Rapport final de l'équipe de révision du WHOIS, les principes du GAC sur le WHOIS, ainsi que par des commentaires reçus de la communauté et le travail de la GNSO pendant les dix dernières années. En outre, il a été demandé à l'EWG d'aborder les questions clés établies par le comité consultatif sur la sécurité et la stabilité (*Security and Stability Advisory Committee* - SSAC) dans son rapport SAC055, et de prendre en considération les opérations et les services Internet actuels et futurs. Le groupe de travail a également évalué les préoccupations des parties qui fournissent, collectent, maintiennent, publient ou utilisent ces données en vertu des attributions de l'ICANN ».

[1] La résolution du Conseil d'administration de l'ICANN est publiée sur : http://www.icann.org/en/groups/board/documents/resolutions-08nov12-en.htm. **L'annexe A** met en lumière la réponse de l'EWG à des questions spécifiques du Conseil d'administration.

2.2 Déclaration d'intention pour guider le travail de l'EWG

Une déclaration d'intention de haut niveau pour guider le travail de l'EWG a été développée. Le groupe pourra ainsi vérifier ses conclusions et ses recommandations comme suit :

Dans le but de soutenir la mission de l'ICANN pour coordonner le système d'identificateurs uniques du système mondial d'Internet et pour assurer l'opération stable et sécurisée du système d'identificateurs uniques d'Internet, l'information sur les noms de domaine gTLD est nécessaire pour promouvoir la confiance du consommateur pour toutes les parties prenantes d'Internet.

En conséquence, il est souhaitable de concevoir un système qui supporte l'enregistrement et la maintenance des noms de domaine, capable de :

- **fournir un accès approprié aux données d'enregistrement exactes, fiables et uniformes**
- **protéger la privacité des informations personnelles**
- **permettre un mécanisme fiable pour identifier, établir et maintenir la capacité de contacter des registrants**
- **supporter un cadre pour aborder les questions qui impliquent les registrants, y compris mais sans s'y limiter : la protection du consommateur, l'investigation sur la cybercriminalité et la protection de la propriété intellectuelle.**
- **fournir une infrastructure pour aborder de manière appropriée les besoins en matière du respect de la loi.**

III. MÉTHODOLOGIE - IDENTIFIER LES UTILISATEURS ET LES OBJECTIFS

3.1 Méthodologie du cas d'utilisation

L'EWG a été encouragé à démarrer son travail « à partir de zéro » pour définir la nouvelle génération des services d'annuaire des données d'enregistrement au lieu d'améliorer le système Whois actuel, qui est largement perçu comme insuffisant. Conformément à la directive du Conseil d'administration, l'EWG a commencé son analyse en étudiant les objectifs existants et potentiels de collecter, stocker et fournir les données d'enregistrement gTLD à un grand nombre d'utilisateurs.

Pour y parvenir, les membres de l'EWG ont travaillé sur un ensemble de cas d'utilisation actuels impliquant le système WHOIS en vigueur, en analysant chacun d'eux pour identifier (i) les utilisateurs qui veulent accéder aux données, (ii) leurs fondements pour demander cet accès, (iii) les éléments de données dont ils ont besoin et (iv) les objectifs qui seront remplis par ces données. Les cas ont été également utilisés pour identifier toutes les parties prenantes impliquées dans la collecte, le stockage et la provision des données d'enregistrement ; cela a aidé à l'EWG à comprendre les flux de travail existants et potentiels et la manière de mieux satisfaire les besoins des utilisateurs par le biais d'un RDS de nouvelle génération.

Ces cas d'utilisation, qui ont illustré un large éventail d'utilisateurs, de besoins et de flux de travail, n'étaient pas censés être exhaustifs mais plutôt représentatifs du grand nombre d'utilisateurs du WHOIS actuel. Un inventaire des cas d'utilisation utilisés par l'EWG se trouve dans l'**Annexe B**.

L'EWG a analysé tous ces cas d'utilisation et en a tiré des leçons qui lui ont servi pour identifier un ensemble consolidé de parties prenantes et d'objectifs

souhaitables qui devraient être traités par le RDS, ainsi qu'un ensemble d'utilisations abusives potentielles que le système devrait être en mesure de prévenir (détaillées dans la prochaine section de ce rapport).
En outre, l'EWG a consulté des documents de référence sur les activités préalables concernant le Whois, les commentaires de la communauté et des cas d'utilisation pour analyser les besoins spécifiques de chacun des domaines indiqués dans la figure 1 ci-dessous.

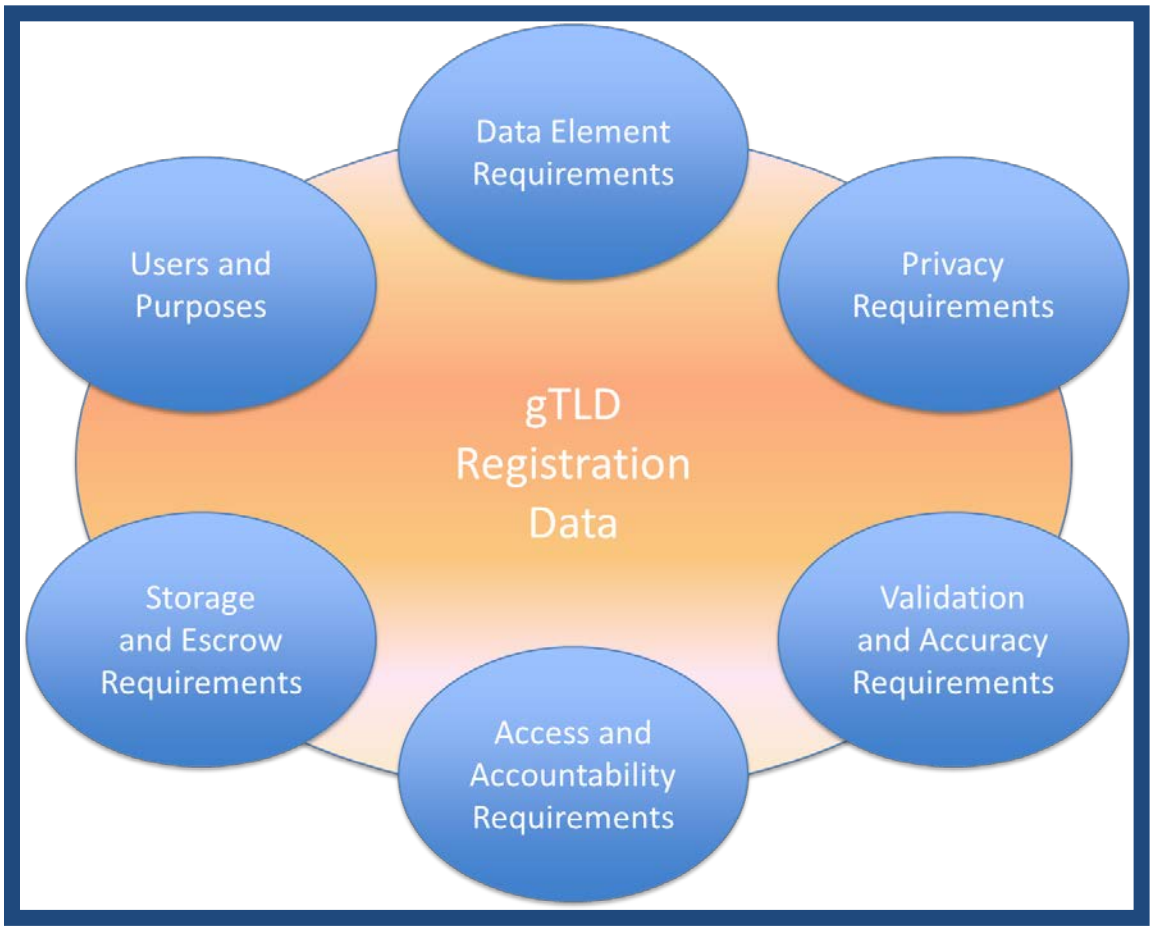

Figure 1 : Besoins d'analyse

L'EWG espère continuer son travail en analysant les fins et les besoins pour obtenir le nombre minimal de données, risques associés, implications sur la politique et les lois de privacité et d'autres questions qui devraient être mieux analysées dans la version finale provisoire de ce rapport.

3.2 Identifier les utilisateurs du RDS

L'EWG a analysé chacun des cas d'utilisation représentatifs pour développer le tableau suivant, qui synthétise les types d'utilisateurs qui veulent accéder aux données d'enregistrement gTLD, les fondements du besoin d'accès et les objectifs généraux desservis par ces données. Vous trouverez plus de détails sur chaque cas d'utilisateur et les interactions de l'utilisateur avec le RDS dans l'**Annexe B**.

Utilisateur	But	Exemples de cas d'utilisation	Fondements pour l'enregistrement des données d'accès
Tous les registrants (par ex., personnes physiques, personnes morales, fournisseurs des services proxy/de confidentialité)	Contrôle du nom de domaine	Création d'un compte pour l' enregistrement de noms de domaine	Permettre l'enregistrement de noms de domaine par tout registrant que crée un nouveau compte avec un bureau d'enregistrement
		Surveillance de la modification de données des noms de domaine	Détecter la modification accidentelle, non-informée ou non-autorisée des données d'enregistrement d'un nom de domaine
		Gestion du portefeuille des noms de domaine	Faciliter la mise à jour des données d'enregistrement d'un nom de domaine (par ex., contacts désignés, adresses) pour maintenir un portefeuille de noms de domaine
		Transferts de noms de domaine	Permettre le transfert d'un nom de domaine initié par un registrant à un autre bureau d'enregistrement
		Suppressions des noms de domaine	Permettre la suppression d'un nom de domaine expiré
		Nom de domaine Mises à jour du DNS	Permettre le changement de DNS d'un nom de domaine initié par le registrant
		Renouvellement des noms de domaine	Permettre le renouvellement d'un nom de domaine enregistré par le contact de facturation du nom de domaine (un individu ou une entité)
		Validation du contact du nom de domaine	Faciliter la validation initiale et continue des données d'enregistrement d'un nom de domaine (par ex., contacts désignés, adresses)
Registrants protégés (par ex. clients des services proxy/de confidentialité)	Protection des données personnelles	Protection améliorée des enregistrements	Permettre l'utilisation des services d'enregistrement proxy/de confidentialité accrédités par tout registrant cherchant à minimiser l'accès public aux données et aux adresses personnelles.
		Protection maximale des enregistrements	Permettre l'utilisation de services d'enregistrement proxy accrédités par des individus ou des groupes menacés,

Utilisateur	But	Exemples de cas d'utilisation	Fondements pour l'enregistrement des données d'accès
			utilisant des identificateurs sans visibilité issus d'un tiers de confiance
Personnel technique d'Internet (par ex., administrateurs du DNS, administrateurs du courriel, administrateurs Web)	Résolution des problèmes techniques	Contact avec le personnel technique des noms de domaine	Faciliter le contact avec le personnel technique (individus ou entités) pouvant aider à résoudre des questions techniques ou opérationnelles des noms de domaine (par ex., résolution de défaillances du DNS, questions liées au service de courriel, questions fonctionnelles du site Web)
Fournisseurs de services en ligne (par ex. ISP, fournisseurs d'hébergement, autorités de certification (CA), services de réputation.	Provision de services Internet	Contact avec le registrant du nom de domaine	Permettre de rétablir le contact avec un client (individu ou entité) pour aborder les questions commerciales d'un nom de domaine lorsque la méthode de contact habituelle avec le fournisseur ne fonctionne pas
		Services réputés en matière de noms de domaine	Permettre l'analyse de la liste blanc/noir des noms de domaine par des fournisseurs de services réputés
		Services de certification des noms de domaine	Aider l'autorité de certification (CA) à identifier le registrant d'un nom de domaine lié à un certificat SSL/TLS
Utilisateurs individuels d'Internet (par ex. consommateurs)	Utilisation individuelle d'Internet	Contact avec le monde réel	Aider les consommateurs à obtenir une information de contact non-Internet pour le registrant du nom de domaine (par ex. adresse commerciale)
		Protection du consommateur	Disposer d'un mécanisme simple pour que les consommateurs puissent contacter les registrants de noms de domaine (par ex., les détaillants en ligne) afin de résoudre les problèmes rapidement, sans l'intervention de LEA/OpSec.
		Action légale / civile	Aider les victimes individuelles à identifier le registrant du nom de domaine impliqué dans des activités illégales potentielles pour permettre une enquête ultérieure de LEA/OpSec.
Utilisateurs commerciaux d'Internet (par ex. détenteurs de marques, courtiers,	Achat/vente commerciale des noms de domaine	Vente de noms de domaine par un intermédiaire	Permettre la diligence due liée à l'achat d'un nom de domaine
		Analyse des risques d'un nom de domaine (*Trademark Clearance*)	Permettre l'identification des registrants de noms de domaine pour supporter l'analyse des risques lors de l'établissement de nouvelles marques
		Acquisition de noms de	Faciliter l'acquisition d'un nom de

Utilisateur	But	Exemples de cas d'utilisation	Fondements pour l'enregistrement des données d'accès
agents)		domaine	domaine enregistré au préalable en permettant le contact avec le registrant
		Demande d'achat d'un nom de domaine	Permettre de déterminer la disponibilité d'un nom de domaine et le registrant actuel (s'il y en avait)
		Nom de domaine Historique des enregistrements	Fournir l'historique de l'enregistrement de noms de domaine pour identifier les anciens registrants et les dates
		Noms de domaine pour des registrants spécifiques	Permettre de déterminer tous les noms de domaine enregistrés par une entité spécifique (par ex., fusion/création de la vérification des actifs)
Chercheurs d'Internet	Recherche de noms de domaines	Nom de domaine Historique des enregistrements	Permet la recherche et l'analyse statistique des enregistrements de noms de domaine (également utile pour les utilisateurs commerciaux d'Internet)
		Noms de domaine pour des registrants spécifiques	Permet la recherche et l'analyse statistique des registrants de noms de domaine (également utile pour les utilisateurs commerciaux d'Internet)
		Contact du registrant d'un nom de domaine	Permet de faire des sondages sur les registrants de noms de domaine (aussi utile pour les fournisseurs de services en ligne)
Titulaires de droits de propriété intellectuelle (par ex., propriétaires de marques commerciales, propriétaires d'IP)	Actions légales	Fournisseur de services proxy Identification du client	Permettre d'identifier le client des services proxy associé à un nom de domaine sous enquête pour de possibles violations ou vol d'IP (c'est à dire, révélation)
		Nom de domaine Contact de l'utilisateur	Permettre le contact avec la personne utilisant un nom de domaine faisant l'objet d'une enquête à cause de la violation des marques de commerce ou du vol des IP
		Combattre l'utilisation frauduleuse des données d'enregistrement	Faciliter l'identification et répondre à l'utilisation frauduleuse de données légitimes (par ex., adresse) appartenant à un autre registrant
Chercheurs Non-LEA (*Law Enforcement Agencies*) Par ex., autorités fiscales, fournisseurs UDRP,	Application règlementaire et contractuelle	Enquête fiscale en ligne	Faciliter l'identification des noms de domaine engagés dans les ventes en ligne par les autorités fiscales nationales, provinciales ou locales
		Procédures UDRP	Laisser que les fournisseurs UDRP confirment le défendeur d'un nom de domaine, réalisent des vérifications de la conformité, déterminent les exigences des processus juridiques et le protègent contre le « cyberflight »

Utilisateur	But	Exemples de cas d'utilisation	Fondements pour l'enregistrement des données d'accès
conformité de l'ICANN)		Conformité contractuelle du RAA	Laisser que la conformité contractuelle de l'ICANN réalise les audits et réponde aux plaintes concernant la conduite des bureaux d'enregistrement (par ex., inexactitude ou non-disponibilité des données, décision de mise en œuvre de l'UDRP, transfert de plaintes, rétention et dépôt de données)
Chercheurs LEA/OpSec (par ex., organismes d'application de la loi, équipes de réponse aux incidents)	Réduction des abus	Examiner les noms de domaine abusifs	Permettre l'analyse efficace et les évidences recueillies par le personnel de LEA/OpSec en réponse à l'enregistrement possiblement malicieux d'un nom de domaine
		Point de contact pour les abus des noms de domaine en danger	Assister à la rémédiation des noms de domaine en danger en aidant le personnel LEA/OpSec à contacter le registrant ou responsable des abus/ISP désigné
Scélérats (par ex., ceux responsables du spam, des attaques de déni de service distribué (DDoS), du hameçonnage, du vol d'identité, du piratage des domaines)	Activités malveillantes sur Internet	Piratage du nom de domaine	Obtenir les données d'enregistrement du nom de domaine pour accéder de manière illicite au compte du registrant et détourner le/s nom/s de domaine de ce registrant
		Enregistrement malveillant d'un nom de domaine	Utiliser un compte d'enregistrement d'un nom de domaine en danger/existant pour enregistrer de nouveaux noms afin de supporter des activités criminelles, frauduleuses ou abusives
		Fouille des données d'enregistrement pour Pourriel/Escroquerie	Obtenir les données d'enregistrement d'un nom de domaine pour son utilisation malveillante par des spammeurs, des escrocs et d'autres criminels (scélérats)

Tableau 1. Utilisateurs

La figure 2 montre un résumé non exhaustif des utilisateurs du système Whois actuel, y compris ceux dont les fins sont constructives et malicieuses. Conformément au mandat de l'EWG, tous ces utilisateurs ont été examinés pour identifier les futurs flux de travail existants et possibles, les parties prenantes et les données impliquées.

Figure 2 : Utilisateurs

Dans ce rapport, le terme « requérant » est utilisé pour décrire génériquement tous les utilisateurs qui souhaitent obtenir les données d'enregistrement gTLD du système. Tel qu'il est détaillé dans la section IV ci-dessous, l'EWG recommande d'abandonner le modèle du Whois actuel (ainsi que le protocole) qui donne à tous les utilisateurs le même accès public anonyme (trop souvent inexact) aux données d'enregistrement gTLD. Au lieu du Whois, l'EWG recommande un changement de paradigme selon lequel les données d'enregistrement sont collectées, validées et divulguées seulement à des fins admissibles, avec certains éléments de données accessibles seulement aux demandeurs authentifiés qui sont tenus responsables de l'usage approprié.

3.3 Identifier les objectifs à adopter ou à interdire

L'EWG a cherché à donner la priorité aux fins énumérées dans la section 3.2 pour se cibler sur le développement des cas d'utilisation et réduire l'univers des objectifs admissibles. Toutefois, il a été difficile d'établir les fondements pour répondre aux besoins de quelques utilisateurs qui utilisent le système actuel du

Whois à l'heure actuelle mais pas d'autres, tant que leurs fins ne soient pas illicites. Ce résultat a amené l'EWG à recommander que toutes les fins identifiées dans la section 3.2 répondent en quelque sorte aux besoins du RDS, exception faite des activités illicites connues sur Internet qui devraient être activement découragées. Les objectifs admissibles recommandés par l'EWG sont résumées ci-dessous.

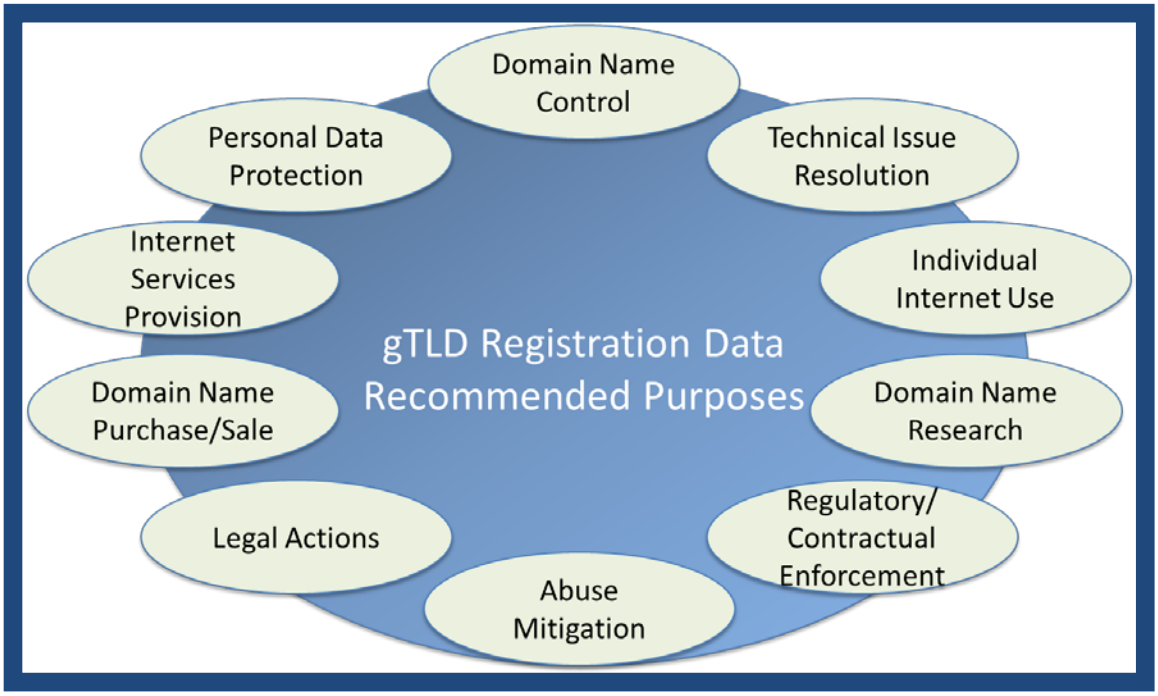

Figure 3 : Objectifs poursuivis

Il faut signaler que chaque objectif contient un grand nombre de cas d'utilisation actuels ou futurs. Bien que l'EWG ne soit pas parvenu à identifier tous les cas d'utilisation possibles, il s'est efforcé d'explorer un échantillon représentatif dans le but d'identifier les types d'utilisateurs, ainsi que leurs fins ou objectifs, voulant accéder aux données d'enregistrement gTLD. Toutefois, le RDS devrait être conçu avec la capacité d'accueillir les nouveaux utilisateurs et les objectifs admissibles qui pourraient apparaître au fil du temps.

3.4 Parties prenantes impliquées dans le RDS

Le tableau suivant fournit un résumé représentatif de l'ensemble des parties prenantes concernées dans la collecte, enregistrement, divulgation et utilisation des données d'enregistrement des gTLD, appliquées aux objectifs associés Certaines parties prenantes fournissent des données (par ex., les registrants), alors que d'autres collectent/entreposent des données (par ex., les registres et les bureaux d'enregistrement) ou divulguent des données (par ex., l'opérateur RDS, les fournisseurs de services proxy/de confidentialité). Toutefois, la plupart des parties prenantes sont des parties impliquées dans le démarrage de nouvelles demandes de données (par ex., les propriétaires de marques, leurs agents) ou des parties identifiées, contactées ou impactées par les données divulguées (par ex., cas d'abus du nom de domaine). Ce résumé vise à illustrer l'ensemble des parties prenantes les plus susceptibles d'être affectées par le RDS. Toutefois, dans toute transaction impliquant les données d'enregistrement, il doit y avoir bien d'autres parties prenantes qui ne sont pas énumérées ici.

Parties prenantes	Objectifs
Cas d'abus des noms de domaine	Réduction des abus
Acheter une société	Achat/vente des noms de domaine commerciaux
Acquisition des agents/avocats de la société	Achat/vente des noms de domaine commerciaux
Service de validation d'adresses	Contrôle du nom de domaine
Agents du registrant	Contrôle du nom de domaine
Propriétaire de marques	Exécution des contrats/règlementation
Fournisseur de services de gestion de marques	Contrôle du nom de domaine
Propriétaire de marques	Achat/vente des noms de domaine commerciaux
Autorité de certification	Provision de services Internet
Plaignant	Exécution des contrats/règlementation
Consommateurs utilisant des sites Web	Utilisation individuelle d'Internet
Intermédiaire d'un domaine	Achat/vente des noms de domaine commerciaux
Acheteur d'un domaine	Achat/vente des noms de domaine commerciaux
Victime de fraude	Actions légales
Agent de la victime de fraudes	Actions légales
Personnel de l'agence gouvernementale	Exécution des contrats/règlementation
Conformité de l'ICANN	Exécution des contrats/règlementation
Fournisseurs de services Internet	Réduction des abus
Rechercheur	Utilisation individuelle d'Internet
Personnel des organismes d'application de la loi	Actions légales pour réduire les abus
Liste des contacts	Provision de services Internet

Fournisseur de services en ligne	Provision de services Internet
Fournisseurs de services Op/Sec	Réduction des abus
Étude de l'organisation de parrainage	Recherche de noms de domaines
Personne/entité faisant l'objet d'une recherche	Exécution des contrats/règlementation
Service client des services proxy / de confidentialité	Achat/vente des noms de domaine commerciaux Contrôle des noms de domaine Provision de services Internet Exécution des contrats/règlementation Protection des données personnelles
Fournisseur de services proxy / de confidentialité	Réduction des abus Achat/vente des noms de domaine commerciaux Contrôle des noms de domaine Recherche de noms de domaine Provision de services Internet Actions légales Protection des données personnelles Exécution des contrats/règlementation Résolution des questions techniques
Opérateur RDS	Toutes fins
Registrant ou titulaire de nom de domaine	Toutes fins
Agent du registrant	Achat/vente des noms de domaine commerciaux Provision de services Internet Exécution des contrats/règlementation
Bureau d'enregistrement	Achat/vente des noms de domaine commerciaux Contrôle des noms de domaine Recherche de noms de domaine Utilisation individuelle d'Internet Provision de services Internet Actions légales Protection des données personnelles Exécution des contrats/règlementation Résolution des questions techniques Réduction des abus
Registre	Toutes fins
Rapporteur du problème	Résolution des problèmes techniques
Chercheur	Recherche de noms de domaines
Revendeur	Réduction des abus
Résolveur du problème	Résolution des problèmes techniques
Cible de l'action légale/civile	Utilisation individuelle d'Internet
Contact technique	Résolution des problèmes techniques
Tierces parties cherchant un contact	Actions légales Protection des données personnelles
Agent de confiance	Protection des données personnelles
Membres du panel UDRP	Exécution des contrats/règlementation
Fournisseur UDRP	Exécution des contrats/règlementation
Validateur du besoin accru de protection	Protection des données personnelles
Victime d'abus	Réduction des abus
Fournisseur d'hébergement sur le Web	Résolution des problèmes techniques

Tableau 2. Résumé représentatif des parties prenantes

3.5 Identification des points communs

L'analyse des études de cas d'utilisation faite par l'EWG, a mis en évidence qu'un bon nombre d'utilisateurs ont besoin d'éléments de données similaires, mais pour différentes raisons. Certains besoins sont bien compris, par exemple :

- la capacité de déterminer si un nom de domaine est enregistré
- La capacité de déterminer l'état actuel d'un domaine

Toutefois, certains points en commun ne sont pas accomplis par le système Whois en vigueur de manière uniforme. En voici quelques exemples :

- la capacité de déterminer tous les domaines enregistrés par une entité déterminée
- la capacité de déterminer quand est-ce que le domaine a été enregistré pour la première fois

L'EWG a analysé ces besoins en commun lors du développement des principes recommandés pour guider la conception du RDS. Toutefois, comme il est prévu que les futurs points communs seront identifiés au fil du temps, le système devrait être conçu en ayant à l'esprit son extensibilité.

3.6 Éléments de données identiques à des fins acceptables

L'annexe C décrit les éléments de données pertinents pour chaque objectif admissible. Enfin, quelques-uns de ces éléments de données devraient être collectés pour chaque nom de domaine, alors que d'autres devraient être collectés facultativement pour un sous-ensemble de noms de domaine. En outre, les demandeurs pourront accéder ou non aux éléments de données collectés à travers le RDS. L'EWG espère aborder ces questions plus profondément pour pouvoir faire ses recommandations dans ce domaine mais il recommande une analyse plus poussée des risques et de l'impact sur chaque élément de données pour compléter cette catégorisation. Les commentaires du public aideraient à identifier la manière d'aborder l'analyse des risques et de l'impact, de savoir quel serait le responsable de prendre en charge cette analyse,

et le critère selon lequel chaque élément de données devrait être identifié comme obligatoire ou facultatif, pour collecte et divulgation à travers des méthodes d'accès publiques ou non.

IV. FONCTIONNALITÉS SOUHAITÉES ET PRINCIPES DE CONCEPTION

Sous réserve d'une analyse appropriée de risques et d'impacts, l'EWG considère que la prochaine génération de services d'annuaire de registre (RDS) devrait incorporer les fonctionnalités et les principes de conception suivants :

	Caractéristiques	des principes de conception de l'EWG
4.1	**Pertinence**	
	4.1.1	• Le RDS doit pouvoir s'appliquer à tous les registres gTLD, autant aux existants qu'aux nouveaux. Aucun droit historique ou exemption particulière ne pourraient être accordés.
4.2	**International Considérations**	
	4.2.1 4.2.2	• Une ou plusieurs politiques devraient être établies par chacune des parties prenantes participant au RDS en matière d'accès aux données, d'utilisation et de conservation de données, ainsi qu'en matière de régularité de la procédure. o Ces politiques peuvent varier en fonction des juridictions. o Elles doivent permettre le respect des lois locales. o L'EWG envisage d'approfondir l'analyse de ces questions. • Pour avoir une portée vraiment mondiale, le RDS devrait prévoir l'affichage des données d'enregistrement en plusieurs langues, scripts et jeux de caractères) o Des analyses supplémentaires doivent être encore mises en place par les experts IDN pour définir ces conditions.
4.3	**Responsabilité**	
	4.3.1 4.3.2	• Toutes les parties de l'écosystème de noms de domaine possèdent des responsabilités par rapport aux autres. • Les registrants ont la responsabilité de fournir

	4.3.3 4.3.4 4.3.5 4.3.6	et de tenir à jour des données d'enregistrement actuelles, exactes et opportunes dans le RDS. • Les registrants ont la responsabilité d'assurer la possibilité que l'on puisse contacter la personne concernée pour résoudre de manière rapide tout problème qui pourrait survenir au niveau de la connexion de son nom de domaine. • Les registrants devraient assumer l'entière responsabilité de l'enregistrement et de l'utilisation de leurs domaines. • Les bureaux d'enregistrement ont la responsabilité de fournir aux registrants le service spécifié dans leurs contrats, y compris l'accès à des données d'enregistrement mises à jour et exactes. • Des conséquences devraient être prévues en cas de manquement à l'obligation de fournir et de tenir à jour des informations exactes. o L'EWG envisage d'approfondir l'analyse de ces questions.
4.4	**Considérations sur la privacité**	
	4.4.1 4.4.2 4.4.3 4.4.4	• Le RDS devrait tenir compte des besoins en matière de confidentialité, y compris : o un service d'enregistrement comportant des protections accrues destiné à répondre aux besoins généraux en matière de confidentialité des données personnelles ; et o un service d'enregistrement comportant une protection maximale, associée à un service de protection d'accès aux informations par identifiants sécurisés pour des utilisations à risque, liées à la liberté d'expression. • Un système d'accréditation devrait être envisagé pour les fournisseurs de services de confidentialité/proxy, ainsi que des règles pour la fourniture et l'utilisation des services accrédités de confidentialité /proxy.

		• En dehors des noms de domaine enregistrés par le biais de services accrédités de confidentialité/proxy, tous les registrants devraient assumer la responsabilité des noms de domaine qu'ils enregistrent. • L'EWG envisage d'approfondir l'analyse de ces questions, y compris : o Des processus normalisés à mettre en place par tous les fournisseurs accrédités de services de confidentialité/proxy. o Des processus spécifiques liés à la gestion de demandes adressées par des agences d'application de la loi accréditées. o Des processus spécifiques liés à la gestion de demandes adressées par d'autres requérants agréés (par exemple, des titulaires de droits de propriété intellectuelle).
4.5	**Objectifs admissibles**	
	4.5.1 4.5.2	• Des utilisations admissibles /inadmissibles du système devraient être clairement définies. • **La section 3** décrit de manière générale les utilisations admissibles identifiées par l'EWG.
4.6	**Divulgation de données**	
	4.6.1 4.6.2 4.6.3 4.6.4	• Le RDS devrait prévoir la divulgation de données pour des objectifs spécifiques. • Toutes les informations collectées ne seront pas publiques ; leur divulgation dépendra du requérant et de l'objectif poursuivi. • L'accès public à un ensemble minimum de donnés d'identification devrait être disponible, avec certaines restrictions destinées à limiter la collecte en masse d'informations. • Les données s'étant avérées sensibles suite à l'évaluation de risque et d'impact devraient être protégées au moyen d'un accès sécurisé, basé sur : ▪ L'identification d'une utilisation admissible. ▪ La divulgation honnête de l'objectif poursuivi par le

	4.6.5 4.6.6 4.6.7	requérant. ▪ La mise en place d'audits / actions de conformité afin d'assurer que l'accès sécurisé ne fait pas l'objet d'abus. • L'accès à certaines données extrêmement sensibles (conformément aux résultats de l'analyse de risques et d'impact) par le biais de procédures légales spécifiques (par exemple, assignation). • La seule divulgation de données dont l'utilisation est admissible pour l'objectif déclaré. • **L'annexe C** décrit les éléments d'information correspondant à des utilisations admissibles identifiées dans **l'annexe B**.
4.7	**Éléments des données**	
	4.7.1 4.7.2 4.7.3 4.7.4 4.7.5	• Les seuls éléments d'information qui devraient être collectés sont ceux qui font l'objet d'au moins un objectif admissible. • Chaque élément d'information devrait être associé à des objectifs admissibles sur la base des utilisations admissibles identifiées. • La liste des éléments d'information minimum à être collectés, stockés et divulgués publiquement devrait se fonder sur une évaluation de risques. • Afin d'être extensible, le système devrait pouvoir accepter tout élément d'information supplémentaire collecté par les registres, auxquels l'on pourrait accéder par les méthodes et les interfaces d'accès ordinaires. • L'ensemble complet d'éléments d'information devrait être sauvegardé par les registres.
4.8	**Méthodes d'accès**	
	4.8.1	• L'accès ne devrait pas être discriminatoire (c'est à dire, le processus devrait établir

	4.8.2 4.8.3 4.8.4 4.8.5 4.8.6 4.8.7	des règles de jeu équitables pour tous les requérants ayant le même objectif). • Pour décourager des usages inappropriés et pour promouvoir la responsabilité, o tous les accès devraient être authentifiés à un niveau approprié ; et o les requérants souhaitant accéder à des éléments d'information devraient pouvoir demander et recevoir des identificateurs qu'ils pourraient utiliser dans d'autres demandes d'accès authentifié à des données. • Certains types d'accréditation devraient être appliquées aux requérants d'accès sécurisé. o Lorsque les requérants accrédités recherchent des données, leur objectif devrait être [option a] insinué, ou [option b] déclaré à chaque fois qu'une demande est réalisée ?[2] o Différents conditions peuvent être appliquées à différents objectifs. o Si les requérants accrédités enfreignent les conditions établies, des pénalités devraient être appliquées. • Toutes les demandes / réponses devraient protéger la confidentialité et l'intégrité des données en question. • Des services haut de gamme d'accès aux données (par exemple, WHOIS inversé, WhoWas) peuvent être proposés, moyennant certaines modalités d'accréditation. • Toutes les divulgations d'informations devraient se faire par le biais de méthodes d'accès bien définies. L'ensemble complet de données de devrait pas être exporté en masse pour des accès non contrôlés. • La divulgation peut comporter l'affichage

[2] L'EWG envisage d'approfondir l'analyse de ces questions.

		des données ou d'autres méthodes. o Pour faciliter la recherche des données et un accès cohérent, un point d'accès central (par exemple, un portail Web) devrait être proposé. o L'accès à des données publiques devrait être disponible pour tous les requérants, grâce à une méthode d'interrogation anonyme (au moins à travers une page Web). o L'accès sécurisé à des données sensibles devrait être supporté par le Web ou par d'autres méthodes et formats d'accès (par exemple, réponses xml, SMS, courriel), en fonction du requérant et de l'objectif poursuivi. o Les requérants devraient être en mesure d'obtenir des informations fiables en temps réel, si nécessaire.
4.9	**Validation et exactitude**	
	4.9.1 4.9.2 4.9.3	• Pour améliorer la qualité des informations, la syntaxe des données du registrant devrait être validée (c'est à dire, vérifier le format correct [par SAC58]) au moment de la collecte. • Pour améliorer l'utilisation des informations, le nom et les données de contact du registrant devraient être validées du point de vue opérationnel. (c'est à dire, vérifier qu'il soit joignable). • Afin de réduire la fraude o les registrants devraient pouvoir faire une pré-validation, en fournissant un nom/organisation universel unique ainsi que des informations de contact associées avant l'enregistrement initial du nom de domaine. o Une fois que l'exactitude et le caractère unique des données pré-validées sont vérifiés, un code

	4.9.4 4.9.5 4.9.6 4.9.7 4.9.8 4.9.9	d'autorisation (par exemple, PIN) devrait être fourni au registrant. Des noms de domaine comportant un nom/organisation identique ne devraient pas être enregistrés[3] sans qu'un code d'autorisation leur ait été fourni. o L'ICANN devrait conclure un contrat approprié avec un fournisseur tiers pour la mise en place de ce service de pré-validation et la fourniture des codes d'autorisation. • Pour promouvoir la cohérence et l'uniformité, ainsi que pour simplifier la mise à jour des données, o les éléments d'information pré-validés devraient être réutilisables -c'est à dire, applicables à des enregistrements futurs, avec la possibilité de remplacer ces données par défaut en fonction du domaine concerné. o Les mises à jour des éléments d'information pré-validés devraient pouvoir être automatiquement appliquées à tous les noms de domaine liés. • Pour améliorer la qualité, les données de contact /nom du registrant qui n'ont pas été pré-validées devraient l'être d'une manière ou d'une autre (par exemple, implicitement, par le biais d'un paiement réussi par carte de crédit avec nom/contact). • Afin de préserver la rapidité de l'activation tout en promouvant la qualité, le retard dans la validation du nom/contact du registrant ne devrait pas empêcher l'enregistrement réussi et la liste DNS. Or, ces noms de domaine pourraient être signalés et être suspendus/effacés en cas d'échec de la validation au bout d'une période définie.

[3] L'EWG envisage d'approfondir l'analyse de ces questions.

	4.9.10	• Pour permettre une validation globale du nom/contact du registrant, les méthodes de validation opérationnelle ne devraient pas reposer sur une seule méthode de contact (par exemple, l'adresse postale). • Pour préserver la qualité des données au fil du temps, les éléments d'information validés devraient être périodiquement revérifiés -par exemple, lors des mises à jour du nom/contact ou lors du transfert de noms de domaine liés à un nom/contact préalablement validé. • Le système devrait enregistrer si les éléments d'information ont été validés et quand, y compris pour des données qui ne sont jamais divulguées. • Afin de promouvoir l'enregistrement réussi de noms de domaine liés à des informations mises à jour du nom/contact des registrants, ceux-ci devront être informés par rapport à ce processus et aux politiques associées.
4.10.	**Service de validation des normes**	
	4.10.1 4.10.2	• L'utilisation d'un service de validation standard est préférable car : o il réduit les coûts /charges pour les bureaux d'enregistrement/registres. o permet l'utilisation de systèmes plus efficaces de validation de bases de données, tels que la vérification croisée des adresses UPS, les pages jaunes, les corporations/sociétés, les registres des gouvernements, les listes électorales, les registres des agences de renseignements commerciaux, etc. o permet de normaliser, le cas échéant, les procédures de validation pour un pays ou une juridiction spécifiques. o réduit le nombre de recherches en matière de conformité des registres/bureaux d'enregistrement. • L'ICANN devrait conclure un contrat approprié avec un fournisseur tiers de services standard

		de validation afin d'assurer l'exactitude et l'audit des données ainsi que leur disponibilité.
4.11	**Relations contractuelles**	
	4.11.1 4.11.2 4.11.3 4.11.4	• Un fournisseur tiers, véritablement international, devrait prendre en charge l'opération du RDS. • L'ICANN devrait conclure un contrat avec ce fournisseurs tiers du RDS pour rendre possible la conformité, l'audit et la disponibilité. • L'ICANN devrait conclure des contrats appropriés avec le fournisseur de services standard de validation, les fournisseurs de services proxy/de confidentialité, les fournisseurs d'identifiants sécurisés, et d'autres pouvant interagir avec le RDS. • L'ICANN devrait modifier les accords existants (RAA, accords de registre) pour qu'ils s'adaptent au RDS et éliminer ainsi les vieilles exigences.
4.12	**Stockage et exigences du dépôt de données**	
	4.12.1 4.12.2 4.12.3	• Pour maintenir les systèmes redondants et éliminer les points de contact uniques de défaillance, les données devraient être logées dans différents sites (par ex. bureau d'enregistrement, registre, dépôt et RDS). • Les audits devraient être réalisés sur les données déposées afin de vérifier qu'elles soient complètes, tester leur format et leur intégrité. • Le RDS devrait maintenir les éléments de donnés en toute sécurité de sorte de protéger la confidentialité et l'intégrité des éléments de données du risque d'utilisation non autorisée.
4.13	**Coût pour opérer et accéder au RDS**	
	4.13.1	• La question des coûts est un aspect important du RDS. L'EWG espère analyser cette question, y compris les coûts du développement et de l'opération ainsi que les différentes manières de supporter ces dépenses (par ex., absorbées par le

		financement du RDS, compensées par des frais de service à valeur ajoutée).

V. MODÈLE SUGGÉRÉ

Le besoin de collecter, stocker et divulguer des éléments de données exacts pour remplir plusieurs objectifs ont mené l'EWG à proposer un modèle préliminaire pour un RDS de nouvelle génération capable de satisfaire les principes identifiés dans la section 4. Chaque acteur de l'écosystème RDS a différents besoins quant aux données, différents risques, et potentiellement différentes responsabilités. Historiquement, la plupart de ces responsabilités étaient transférées aux bureaux d'enregistrement, dont les objectifs principaux étaient de fournir des noms de domaine opérationnels aux clients payants. L'EWG reconnaît que l'écosystème d'Internet devient de plus en plus complexe, et à partir de l'introduction de centaines de nouveaux gTLD, il semblerait que les nouveaux acteurs devront prendre en charge certaines responsabilités découlant du fait de satisfaire un si large éventail d'objectifs des données d'enregistrement.

Sur la base des fonctionnalités et des principes de conception établis dans la section IV, la figure 4 illustre le modèle recommandé par l'EWG pour la prochaine génération de RDS, où une grande partie de ces principes pourraient être potentiellement incorporés.

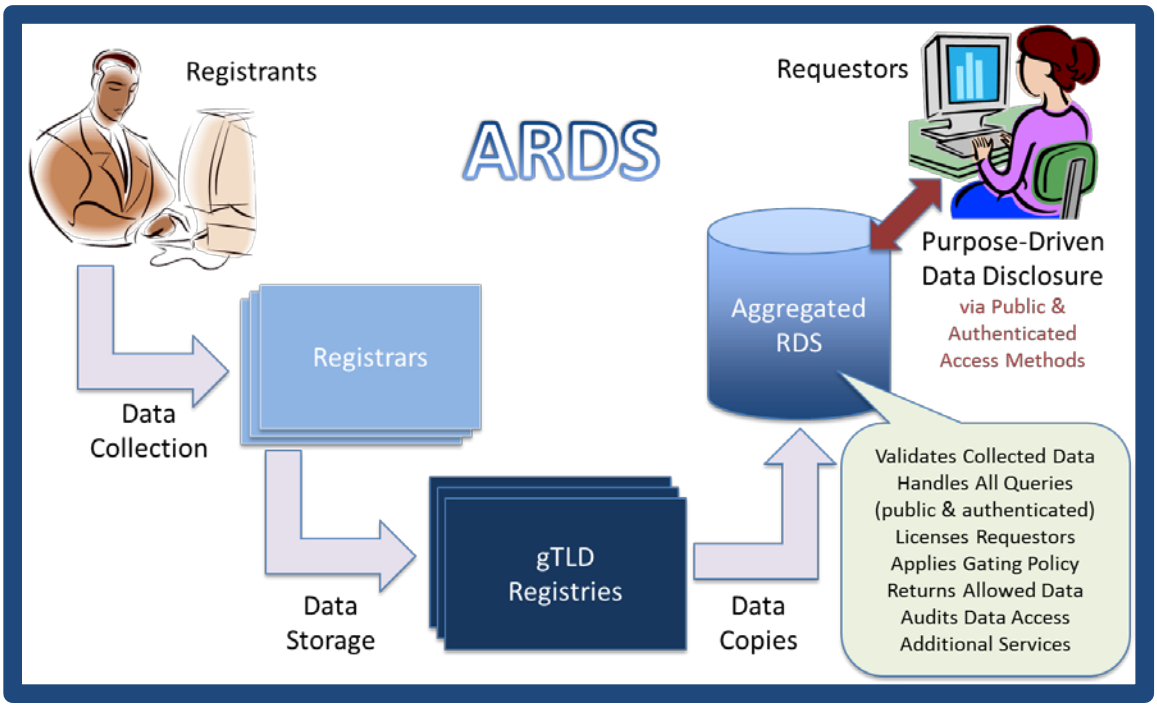

Figure 4. Modèle RDS intégré

5.1 Examen de plusieurs modèles de système

Après avoir identifié les principes recommandés et les fonctionnalités souhaités pour un nouveau RDS, l'EWG a examiné plusieurs modèles alternatifs afin de déterminer la réponse de chacun d'entre eux aux besoins identifiés en matière de données. L'EWG a évalué des systèmes distribués, tels que ceux utilisés actuellement dans le système Whois, ainsi que des systèmes intégrés. L'EWG s'est également penché sur un système de type proxy, où un intermédiaire tiers assure l'accès - mais non pas en tant que référentiel - aux données demandées. Le travail du groupe consultatif sur l'accès aux fichiers de zone (ZFA),[4] qui s'est penché sur des questions similaires dans le contexte du programme des nouveaux gTLD, a été important pour aider l'EWG à bien cerner la question.

[4] Pour plus d'informations, voir les archives du groupe consultatif sur l'accès aux fichiers de zone (ZFA) à : http://archive.icann.org/en/topics/new-gtlds/zone-file-access-en.htm

Les systèmes distribués présentent des défauts qui pourraient être évités avec des modèles alternatifs. Avec des centaines de registres potentiels en ligne, l'EWG a reconnu que la continuité du système distribué qui est actuellement utilisé entraîne des inefficacités et des coûts supplémentaires, dans la mesure où les consommateurs de ces informations sont confrontés à différents formats, informations d'identification, points d'accès, dispositions en matière d'autorisation et d'autres obstacles qui peuvent être créés par le registre ou le bureau d'enregistrement. Tel que signalé par le groupe consultatif ZFA, lorsque « des systèmes d'accès différents sont utilisés, les processus ou les mécanismes d'automatisation mis en œuvre par les consommateurs de fichiers de zone sont plus susceptibles de tomber en panne. Lorsque des erreurs donnent lieu à des pertes d'accès, la résolution du problème peut s'avérer compliquée pour les consommateurs de données, dans la mesure où ils sont obligés d'interagir avec des systèmes de rapport uniques pour résoudre le problème »[5] Ces questions pourraient également s'appliquer au RDS.

En outre, les coûts associés à la modification par les registres et/ou les bureaux d'enregistrement de leurs systèmes afin de créer un nouveau système distribué capable de mettre en place une nouvelle génération de RDS pourrait contraindre l'innovation et l'adoption, étant donné qu'il n'y a apparemment pas d'encouragements financiers ou opérationnels pour soutenir des changements significatifs de la méthode d'accès à ces données. Tel que signalé par le groupe consultatif ZFA :

> « En général, l'accès fiable aux données concernant les fichiers de zone implique des coûts opérationnels et des passifs pour les registres gTLD, sans aucune compensation directe en contrepartie. Puisque cette situation a été acceptée par les opérateurs de registre comme un coût associé à l'exploitation d'un des principaux espaces de noms de domaine

[5] Voir le document de concept du fichier de zone publié sur : http://archive.icann.org/en/topics/new-gtlds/zfa-concept-paper-18feb10-en.pdf

d'Internet, il serait donc logique que les registres réduisent ces coûts s'il existait des moyens plus efficaces d'assurer cet accès. Par exemple, les registres sont tenus de fournir un accès continu à tous, sans qu'aucun accord de niveau de service (SLA) ne soit spécifié. Cela a bien entendu un coût... Le registre est aussi responsable d'assurer une connexion sécurisée et des fichiers de données épurées aux consommateurs de donnés, ce qui engendre des exigences significatives en matière de sécurité pour les registres »[6]

De plus, autant les systèmes distribués que ceux utilisant des proxys rendent difficile, voire impossible, de proposer des fonctionnalités généralement nécessaires, telles que la recherche croisée de registrants TLD, la recherche inverse de registrant de domaine ou même un registre historique de propriété. Toutes ces fonctionnalités pourraient être possibles grâce à une base de données regroupée où soient collectées et mises à jour les informations applicables.

5.2 Proposition d'un RDS intégré

Un modèle intégré de RDS (ARDS) (illustré ci-dessus) a été soutenu par consensus par l'EWG, comme un moyen de répondre aux fonctionnalités souhaitées et aux principes de conception identifiés dans la section 4 ci-dessus.

Dans le modèle proposé :

- L'ADRS sert comme référentiel intégré qui contient une copie ne faisant pas autorité de tous les éléments de données collectés
- Chaque registre gTLD demeure la source officielle sur les données
- Le requérants demandent leurs identifiants d'accès à l'ADRS
- Les registres et les bureaux d'enregistrement sont relevés de l'obligation de fournir les accès du Port 43 ou d'autres dispositions d'accès public.

[6] Pour d'autres considérations, voir le document concept d'accès au fichier de zone.

- Dans la plupart des cas, l'ARDS donne l'accès aux données d'enregistrement en cache, données qui sont copiées des registres gTLD et maintenues à travers des mises à jour périodiques.
- L'ARDS peut aussi fournir l'accès aux données vivantes d'enregistrement obtenues en temps réel des registres gTLD, sur demande. L'ARDS (ou tout autre tierce partie en interaction avec ADRS) sera responsable de l'exécution des services de validation
- L'ARDS est responsable d'auditer l'accès afin de minimiser l'abus et d'imposer des pénalités et d'autres remèdes aux accès inappropriés.
- L'ADRS gère les plaintes sur l'exactitude des données
- ARDS gère la concession de licences pour accéder aux données
- L'ICANN contracte des fournisseurs internationaux externes pour développer et exploiter l'ARDS et supervise la conformité avec les dispositions en vigueur

	Modèle RDS intégré
Avantages	• Évolutivité gérée par un point de contact unique • Améliorations potentielles du transport et de la distribution • Système centralisé pour les demandeurs de données d'enregistrement • Davantage de responsabilité pour la validation et l'accès aux données d'enregistrement (anti-abus) • Capacité de suivi / audit / pénalisation des demandeurs identique à travers de multiples TLD (anti-abus) • Réduction possible de certains coûts actuellement supportés par les registres et les bureaux d'enregistrement pour fournir des données d'accès • La normalisation ou le filtre des données pourraient être fournis • Réduction des exigences de bande passante pour les registres et les bureaux d'enregistrement • Facilitation de la normalisation des approches pour répondre aux préoccupations sur la privacité des

	Modèle RDS intégré
	données locales • Recherche améliorée de la capacité à travers de multiples TLD (comme la recherche inversée) • Minimiser les coûts de transition et de mise en œuvre • Permettre la validation / accréditation des demandeurs qui qualifient pour des objectifs spéciaux (c'est à dire, le respect de la loi) • Faciliter la gestion plus efficace des rapports sur l'inexactitude • Permettre des vérifications aléatoires plus efficaces en matière d'exactitude • Permettre la visualisation d'un portail convivial pour les utilisateurs en une multiplicité de langues, scripts et caractères
Désavantages	• Latence des données • Création d'une source « grandes données » de données informatiques de grande valeur pouvant faire l'objet d'une utilisation abusive potentielle au cas où elles ne seraient pas auditées et maintenues convenablement • Risque accru d'abus interne et d'attaque externe, exigeant une plus grande attention dans la mise en œuvre, les normes et l'audit de la politique de sécurité • Les registres et les bureaux d'enregistrement ne contrôlent plus la distribution des données d'enregistrement

VI. RÉPONDRE À DES INQUIÉTUDES EN MATIÈRE DE CONFIDENTIALITÉ

Une attribution clé de l'EWG concerne la question de l'exactitude des données d'enregistrement. Si la prochaine génération de RDS suppose une plus grande exactitude des données d'enregistrement, un certain nombre de problèmes se posent immédiatement, dont le plus contentieux est peut-être celui de la confidentialité.

L'EWG reconnaît le besoin d'exactitude ainsi que le besoin de protéger la privacité des registrants demandant des protections renforcées de leur information personnelle. Des exemples de registrants éligibles à ces protections accrues incluent des individus ou des groupes menacés, des individus ou des groupes souhaitant exercer leur droit d'expression sur Internet, qui sont largement considérés comme devant être protégés, ou bien des individus dont l'identification mettrait en péril leur vie ou celle de leurs familles.

Conformément aux principes recommandés ayant été énumérés dans la section 4.4, l'EWG a discuté les modalités selon lesquelles le RDS serait en mesure de prendre en compte les besoins des utilisateurs vis-à-vis des risques pour une plus grande protection des services d'enregistrement en utilisant des « identificateurs protégés et sécurisés ». Une option serait l'existence d'une organisation accréditée par l'ICANN et indépendante agissant comme agent de confiance, utilisant un ensemble de critères accordés, qui déterminerait si un registrant qualifie pour une protection maximale. L'EWG espère pouvoir analyser des modèles potentiels d'identificateurs protégés et sécurisés innovants, capables de fournir un équilibre efficace entre la responsabilité et les besoins de privacité des données personnelles des utilisateurs d'Internet vis-à-vis des risques.

VII. IILLUSTRATION DES FONCTIONNALITÉS D'ACCÈS SÉCURISÉ

Le modèle d'accès sécurisé proposé (illustré dans la figure 5) peut être synthétisé de la manière suivante :

- Un sous-ensemble soigneusement sélectionné d'éléments d'informations serait publiquement accessible à des requérants par le biais d'une interface Web[7] du RDS.
- Tous les autres éléments d'informations seraient accessibles à des requérants autorisés uniquement par le biais de méthodes multimodales d'accès sécurisé, supportées par le RDS.
- L'accès sécurisé ne serait disponible que pour les requérants ayant demandé et reçu un identifiant, qu'ils utiliseraient au moment d'authentifier la requête envoyée au RDS. Le processus utilisé pour accorder les identifiants n'est pas défini dans le présent document, mais l'EWG recommande que ce processus tienne compte des raisons invoquée par le requérant pour vouloir accéder aux données d'enregistrement.
- Dans le cadre de l'accès sécurisé, chaque requête devrait identifier l'objectif du requérant autorisé (de façon implicite ou explicite) ainsi qu'une liste des éléments d'information recherchés. Seuls seront communiqués les éléments d'informations disponibles pour le nom de domaine et accessibles pour le requérant en fonction de l'objectif déclaré.

L'EWG espère pouvoir mener un débat sur les méthodes d'accès multi-modal et la manière dont elles pourraient être compatibles avec les protocoles d'accès aux données d'enregistrement actuels ou futurs.

[7] L'EWG s'attend à analyser plus tard la possibilité de faire en sorte que quelques éléments de données d'enregistrement, associées à un nom de domaine du site Web visité, soient accessibles par le biais de l'intégration au navigateur.

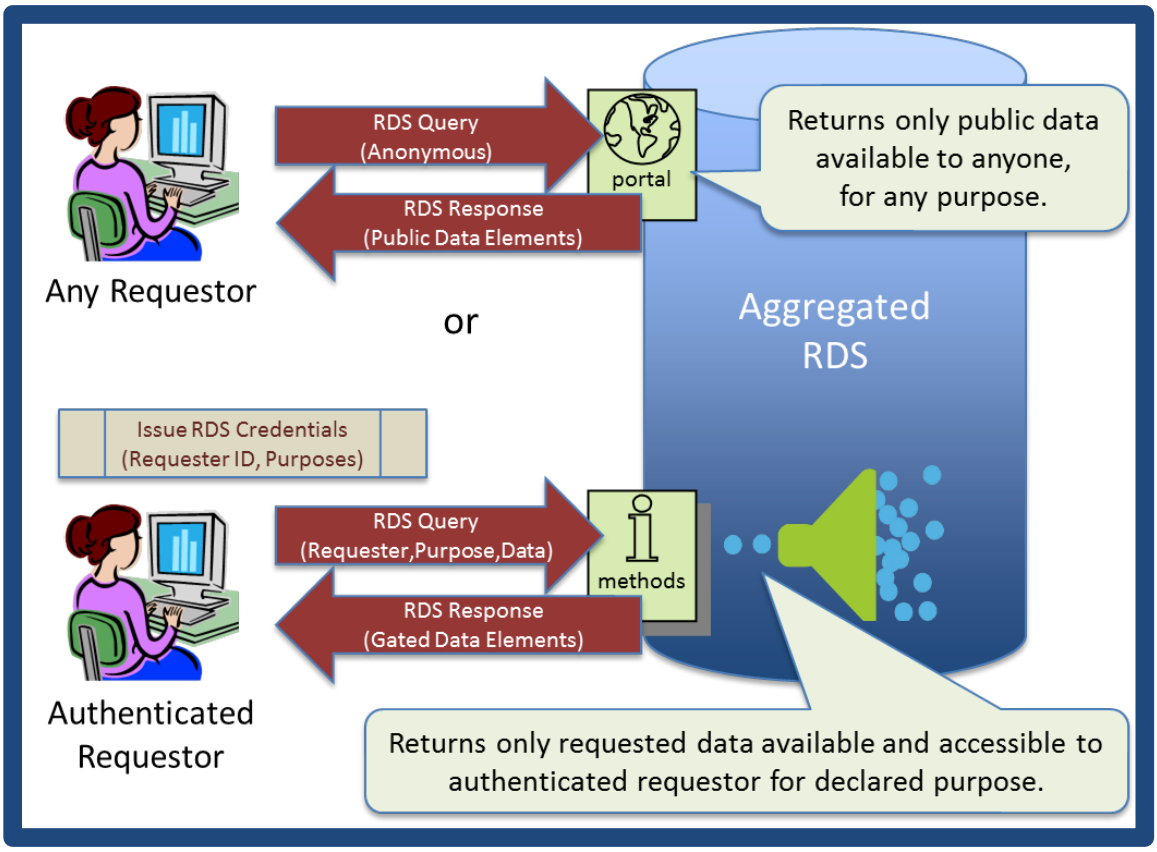

Figure 5. Modèle d'accès sécurisé

VIII. CONCLUSION ET PROCHAINES ÉTAPES

L'EWG suggère l'adoption d'un RDS intégré pour remplacer le système WHOIS actuel afin de répondre aux principes de conception et aux fonctionnalités identifiées par l'EWG et décrites plus en détail dans ce rapport. Cela inclut une fonctionnalité d'« accès sécurisé par identifiant » capable d'assurer une protection de confidentialité accrue pour les registrants à risque, comme ceux exerçant leur droit de libre expression. Le groupe de travail présente aussi des recommandations visant la validation et vérification de l'exactitude des données d'enregistrement collectées, ainsi que le renforcement de la responsabilité grâce à des contrôles d' «accès sécurisé », permettant à des requérants qui souhaitent des informations supplémentaires de demander des identifiants pour accès restreint, sur la base de l'objectif invoqué. Le modèle proposé incorpore des fonctionnalités de responsabilité et d'audit destinées à pénaliser tout usage impropre par des requérants cherchant à accéder à des informations au delà du niveau autorisé.

Il est important de reconnaître que le modèle proposé reflète des compromis âprement obtenus par les membres de l'EWG et ne répond sans doute pas aux attentes de toutes les parties prenantes affectées par le RDS. Cependant, l'EWG espère que ces recommandations seront reconnues comme une amélioration significative par rapport au système actuel de WHOIS.

L'EWG appréciera tout commentaire en ligne ainsi que tout débat de la communauté de l'ICANN à la réunion de Durban sur les questions spécifiques identifiées dans le forum, ainsi que tout autre commentaire sur ce rapport, afin d'enrichir ses délibérations futures. Suite à la consultation publique sur ce rapport, l'EWG se réunira à nouveau afin de réfléchir sur les commentaires reçus et de réviser, le cas échéant, ses recommandations. À l'issue des délibérations de l'EWG, un rapport final sera publié et remis au PDG de l'ICANN et au Conseil d'administration pour servir de base, le cas échéant, aux politiques sur les nouveaux gTLD et aux négociations contractuelles. Tel que spécifié par le

Conseil d'administration, un rapport fondé sur le rapport final sera la base pour la mise en œuvre d'un processus de développement de politiques (PDP) de la GNSO fortement ciblé, initié par le Conseil d'administration.