Rapport final du

Groupe de travail d'experts sur les services d'annuaire gTLD :

Une nouvelle génération de services d'annuaire d'enregistrement (RDS)

STATUT DU PRÉSENT DOCUMENT

Le présent document est le rapport final du groupe de travail d'experts sur les services d'annuaire gTLD (EWG), présentant de façon détaillée nos recommandations au Conseil d'administration de l'ICANN pour une nouvelle génération de services d'annuaire d'enregistrement (RDS) pour remplacer le système actuel du WHOIS.

I. RAPPORT DE SYNTHÈSE 5

II. MANDAT, OBJECTIF ET RESULTATS DE L'EWG 18

a. Mandat 18

b. Objectif 18

c. Résultats 19

III. UTILISATEURS ET OBJECTIFS 22

a. Méthodologie 22

b. Utilisateurs du RDS et objectifs 23

c. Objectifs à desservir ou à interdire 31

d. Parties prenantes impliquées dans le RDS 39

e. Principes des contacts basés sur l'objectif 41

f. Rôles et responsabilités des contacts basés sur les objectifs 43

g. Autorisation d'usage de contact RDS 48

IV. AMELIORER LA RESPONSABILITE 49

a. Principes des éléments de données 50

b. Principes pour l'accès aux données non authentifié et sécurisé 71

c. Principes d'accréditation d'utilisateur du RDS 75

d. Résumé des principaux avantages en matière de responsabilité 81

V. AMELIORER LA QUALITE DES DONNEES 82

a. Exactitude des données et principes de validation 83

b. Processus de pré-validation 86

c. Exactitude, audit et processus de restauration 88

d. Cadre opérationnel pour les ID de contact 89

e. Interaction avec les validateurs 90

f. Principes pour la validation de contact 91

g. Capacité à détenir des données de contact uniques 94

h. Résumé des principaux avantages en matière de qualité des données 94

VI. CONSIDERATIONS JURIDIQUES ET CONTRACTUELLES 97

a. Principes de protection des données 98

b. Principes pour l'accès aux données de la part des représentants de la loi 106

c. Principes de conformité et de relations contractuelles 108

d. Principes de responsabilité et d'audit 108

VII. AMELIORER LA VIE PRIVEE DU TITULAIRE DU NOM DE DOMAINE 114

a. Principes relatifs aux services accrédités d'anonymisation et d'intermédiation 116

b. Principes relatifs aux identifiants sécurisés et protégés 120

c. Résumé des principaux avantages en matière de confidentialité 127

VIII. MODELES DE RDS POSSIBLES 129

a. Principes de conception des modèles 129

b. Les modèles considérés 130

c. Modèle recommandé 130

d. Principes relatifs au stockage, au dépôt fiduciaire et à l'inscription 136

IX. COUTS ET IMPACTS 138

a. Principes relatifs au coût 138

b. Avantages comparés au WHOIS actuel selon le RAA 2013 139

c. Évaluation de risques et d'impact 141

X. CONCLUSIONS ET PROCHAINES ETAPES 143

ANNEXE A : REPONSE AUX QUESTIONS DU CONSEIL 146

ANNEXE B : ÉTUDES EVALUANT LES INSUFFISANCES DU WHOIS 149

ANNEXE C : EXEMPLES DE CAS D'UTILISATION 151

ANNEXE D : OBJECTIFS ET BESOINS DE DONNÉES 154

ANNEXE E : ILLUSTRATIONS D'ACCÈS SÉCURISÉ ET NON AUTHENTIFIÉ 157

ANNEXE F : MODÈLES DE SYSTÈMES CONSIDÉRÉS ET MÉTHODOLOGIE 168

ANNEXE G : CAPACITÉ DES PROTOCOLES EPP ET RDAP À SOUTENIR LE RDS 184

ANNEXE H : MODÈLE ET PRINCIPES POUR LE RELAIS ET LA DIVULGATION 188

ANNEXE I : SCHÉMAS OPÉRATIONNELS DU RDS 193

ANNEXE J : À PROPOS DE L'EWG 195

I. RAPPORT DE SYNTHÈSE

Ce rapport final du groupe de travail d'experts sur les services d'annuaire gTLD (EWG), présente de façon détaillée nos recommandations au président-directeur général et au Conseil d'administration de l'ICANN pour une nouvelle génération de services d'annuaire d'enregistrement (RDS) pour remplacer le système actuel du WHOIS.

Ce rapport final représente le point culminant d'une période intense de plus de 15 mois de travail durant laquelle ce groupe diversifié de bénévoles a passé des milliers d'heures sur des recherches approfondies, a pris en considération plus de 2600 pages de commentaires publics, de réponses aux enquêtes et de résultats de recherches, et a participé à 19 consultations publiques de la communauté, 35 jours de réunions de l'EWG en personne, 42 téléconférences de l'EWG, plus de 200 téléconférences avec les sous-équipes et sans compter les sessions de collecte d'informations avec des experts externes et des membres de la communauté, tout cela pour répondre à une simple question :

Est-ce qu'il y a une alternative au WHOIS actuel afin de mieux desservir la communauté Internet mondiale ?

Oui, il y en a une. L'EWG a recommandé de manière unanime l'abandon du modèle WHOIS actuel qui donne à chaque utilisateur le même accès public entièrement anonyme (souvent inexact) aux données d'enregistrement des gTLD.

À la place, l'EWG recommande une révolution conceptuelle vers une nouvelle génération de RDS qui collecte, valide et divulgue les données d'enregistrement des gTLD uniquement à des fins autorisées.

Alors que les données de base resteraient disponibles au public, le reste serait accessible uniquement aux demandeurs accrédités qui s'identifient eux-mêmes, énoncent leurs objectifs, et acceptent d'être tenus responsables pour une utilisation appropriée.

Les pages suivantes dont le nombre dépasse les 150 décrivent les contributions et les recherches qui ont mené l'EWG à ces recommandations, une proposition détaillée pour un nouveau RDS, ainsi que les conclusions suivantes :

- Cette question est très complexe.
- L'EWG a examiné cette question à partir d'une multitude de perspectives et a conduit des recherches afin de s'assurer que le RDS proposé soit applicable.

- Le RDS proposé, bien qu'il ne soit pas parfait, reflète avec attention les compromis équilibrés et réalisés avec des éléments inter-dépendants qui ne devraient pas être séparés.
- Le RDS proposé est conçu pour aborder de front, et d'une manière sans précédent :
    - les questions complexes relatives à la vie privée ;
    - les défis de validation qui ont longtemps dégradé la qualité et l'exactitude des données ; et
    - atteindre un équilibre réalisable entre l'accès et la responsabilité.
- Le RDS devrait être adopté dans son ensemble. L'adoption de certains mais pas tous les principes de conception recommandés dans ce rapport réduit les bénéfices pour l'écosystème entier.

Le présent rapport final, y compris les recommandations et les principes proposés pour la nouvelle génération de RDS, reflète un consensus. Ce soutien est remarquable étant donné le large éventail de perspectives et de parties prenantes reflété parmi les membres de l'EWG.[1]

L'EWG est certain que le présent rapport final répond aux directives du Conseil de l'ICANN pour aider à redéfinir l'objectif et les dispositions en matière de données d'enregistrement des gTLD fournissant une base solide pour aider la communauté de l'ICANN (à travers l'organisation de soutien des noms génériques, GNSO) à créer une nouvelle politique mondiale pour les services d'annuaire gTLD.

L'EWG est certain que le RDS décrit dans le présent rapport final apporte une base plus solide que celle qui existe aujourd'hui, une base à partir de laquelle la GNSO peut développer une nouvelle politique mondiale pour les données d'enregistrement des gTLD afin de protéger la vie privée et assurer une plus grande exactitude, responsabilité et transparence pour l'écosystème ICANN entier pour les années à venir.

Durant l'examen du présent rapport final par le Conseil d'administration, la GNSO et la communauté de l'ICANN, l'EWG recommande que la prise en considération soit encadrée par les questions suivantes :

- Est-ce que le RDS est préférable à l'actuel WHOIS ?

[1] Voir l'annexe J pour la composition de l'EWG et l'expertise des membres.

- Si la réponse est non, est-ce que la communauté de l'ICANN est d'accord avec le fait que le système WHOIS actuel devrait continuer, et peut-il répondre aux besoins de l'Internet mondial en évolution ?

Contexte

L'EWG a été établi par le président-directeur général de l'ICANN, Fadi Chehadé, à la 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.[2]

Pour aller au-delà des faiblesses du système WHOIS identifiées par de nombreux rapports de la communauté et études[3], le mandat du groupe de travail est de réexaminer et de définir l'objectif de la collecte et du maintien des données d'enregistrement des gTLD, de considérer la manière de sauvegarder les données, et de proposer une solution de nouvelle génération pouvant mieux répondre aux besoins de la communauté Internet mondiale.

En commençant par faire table rase, l'EWG a remis en question les hypothèses fondamentales sur les objectifs, utilisations, collecte, maintien et mise à disposition des données d'enregistrement. L'EWG a pris en considération chacune des parties prenantes concernées par les services d'annuaire des gTLD, examinant leurs besoins en exactitude, accès et vie privée. Il a pris en considération d'éventuelles approches pour répondre à ces besoins de manière plus efficace.

Pour orienter ses délibérations, l'EWG a développé une déclaration d'intention de haut-niveau, en l'utilisant afin d'aligner les recommandations de ce rapport avec la mission de l'ICANN et de concevoir un système pour soutenir l'enregistrement et le maintien des noms de domaine qui :

[2] Se référer à https://www.icann.org/news/announcement-2-2012-12-14-en

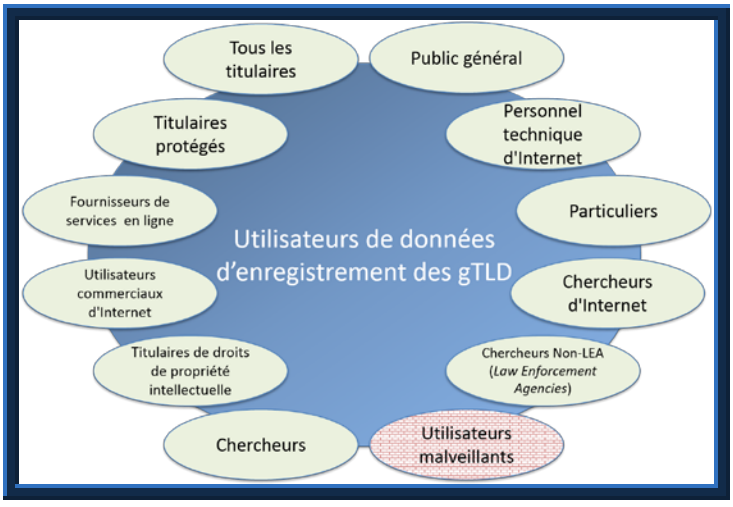
[33] Se référer à l'annexe B pour une liste des rapports qui présentent les faiblesses du WHOIS.

- fournit un accès approprié aux données d'enregistrement exactes, fiables et uniformes ;
- protège le caractère privé des informations des titulaires ;
- permet un mécanisme fiable pour identifier, établir et maintenir la capacité à contacter des titulaires de noms de domaine ;
- soutient un cadre pour aborder les questions qui impliquent les titulaires de noms de domaine, y compris mais sans s'y limiter : la protection du consommateur, les enquêtes sur la cybercriminalité et la protection de la propriété intellectuelle ; et
- fournit une infrastructure pour aborder de manière appropriée les besoins en matière de respect de la loi.

Utilisateurs et objectifs

L'EWG a examiné les objectifs actuels et potentiels pour la collecte, le stockage, et la fourniture des données d'enregistrement gTLD pour une large variété d'utilisateurs, examinant un vaste et représentatif ensemble d'actuels cas d'utilisation du WHOIS.

L'EWG a pris en considération la totalité de ces cas d'utilisation et des leçons apprises de ceux-ci, ainsi que les documents de référence et les contributions de la communauté, pour obtenir un ensemble consolidé d'utilisateurs et d'objectifs admissibles par le RDS et les éventuelles mauvaises utilisations qui doivent être décourageées.



Objectifs à desservir ou à interdire

Conformément au mandat de l'EWG, tous ces utilisateurs ont été interrogés pour identifier les futurs flux de travail existants et possibles, les parties prenantes et les données impliquées.

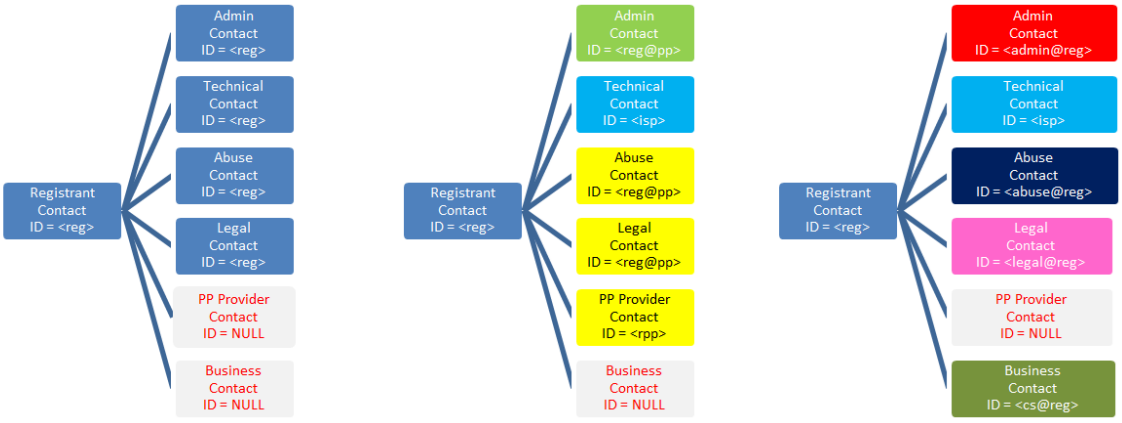
Les besoins liés aux informations d'enregistrement de noms de domaine ont été analysés afin d'en retirer des éléments de données obligatoires, liés aux risques, aux lois relatives à la vie privée et aux implications politiques, et répondre à d'autres questions étudiées dans ce rapport. Les objectifs admissibles recommandés par l'EWG sont résumés ci-contre.

Les objectifs admissibles actuellement identifiés et les données d'enregistrement associées, les contacts et les besoins des demandes sont définis ci-après et détaillés dans la section III.

Objectif	comprend des tâches telles que…
Contrôle du nom de domaine	Créer, gérer et surveiller un nom de domaine propre à un titulaire, y compris la création du nom de domaine, la mise à jour d'informations à propos du nom de domaine, le transfert du nom de domaine, le renouvellement du nom de domaine, la suppression du nom de domaine, le maintien d'un portefeuille de nom de domaine, et la détection d'usage frauduleux des informations de contact propre au titulaire.
Protection des données personnelles	Identifier le fournisseur de services d'intermédiation / d'anonymisation accrédité ou l'approbateur de l'accès sécurisé par identifiant associés au nom de domaine et rapporter les abus, demander la révélation ou la prise de contact avec le fournisseur.
Résolution des problèmes techniques	Travailler pour résoudre les problèmes techniques associés à l'utilisation d'un nom de domaine, y compris les problèmes de distribution d'e-mail, la résolution de défaillances du DNS, et les problèmes fonctionnels de site Internet, en contactant le personnel technique chargé de s'occuper de ces questions.
Certification des noms de domaine	L'autorité de certification (CA) en délivrant un certificat X.509 à un sujet identifié par un nom de domaine ayant besoin de confirmer que le nom de domaine est enregistré auprès du sujet certifié.

Objectif	comprend des tâches telles que…
Utilisation individuelle d'Internet	Identifier l'organisation utilisant un nom de domaine pour créer un climat de confiance avec le consommateur, ou contacter cette organisation pour lui porter une plainte d'un client ou déposer une plainte contre cette organisation.
Achat ou vente des noms de domaine commerciaux	Réaliser des enquêtes d'achat à propos d'un nom de domaine, acquérir un nom de domaine d'un autre titulaire et permettre un processus de recherche raisonnable.
Recherche du DNS d'intérêt public/académique	Les études de recherche d'intérêt public et académique à propos des noms de domaine publiés dans le RDS, y compris des informations publiques concernant le titulaire et les contacts désignés, l'histoire et le statut du nom de domaine, et les noms de domaine enregistrés par un titulaire donné.
Actions en justice	Rechercher d'éventuels usages frauduleux de nom ou d'adresse d'un titulaire par d'autres noms de domaine, rechercher d'éventuelles atteintes aux marques déposées, contacter un représentant juridique du titulaire/détenteur de licence avant d'intenter des poursuites judiciaires et ensuite, intenter des poursuites judiciaires si le problème n'est pas résolu de manière satisfaisante.
Exécution des contrats/règlementation	Enquête commerciale des autorités fiscales avec une présence en-ligne, une enquête UDRP (politique uniforme de règlement de litiges relatifs aux noms de domaine), enquête de conformité contractuelle, et audit de dépôt fiduciaire des données d'enregistrement.
Enquête policière & réduction des abus de DNS	Rapporter les abus à une personne qui peut enquêter et traiter ces abus, ou contacter les entités associées à un nom de domaine pendant une enquête policière autonome.
Transparence du DNS	Demander les données d'enregistrement rendues publiques par les titulaires afin de répondre à une large variété de besoins d'informer le public général.

Pour fournir un accès aux données d'enregistrement basé sur les objectifs tout en améliorant la communication et la vie privée, l'EWG a développé des principes pour des contacts basés sur les objectifs (PBC). Soutenus par des rôles et des responsabilités définis, les PBC ont été attribués à tous les objectifs admissibles où l'on a besoin de contact. Trois exemples sont illustrés ci-dessous et présentés en détail dans les sections III et IV.



L'EWG a analysé de manière plus approfondie tous les éléments de données d'enregistrement, en commençant par ceux définis dans le RAA 2013, pour en retirer un ensemble de principes directeurs pour la collecte et la divulgation de données qui concorde avec le cadre recommandé des PBC, ainsi qu'avec les recommandations faites pour rester en conformité avec les lois de protection des données. L'EWG a formulé des recommandations approfondies afin d'identifier de nouveaux éléments de données que les titulaires et les contacts peuvent choisir de publier pour rendre la communication plus solide. Ces recommandations sont présentées en détail dans la section IV et des exemples sont donnés à l'annexe E.

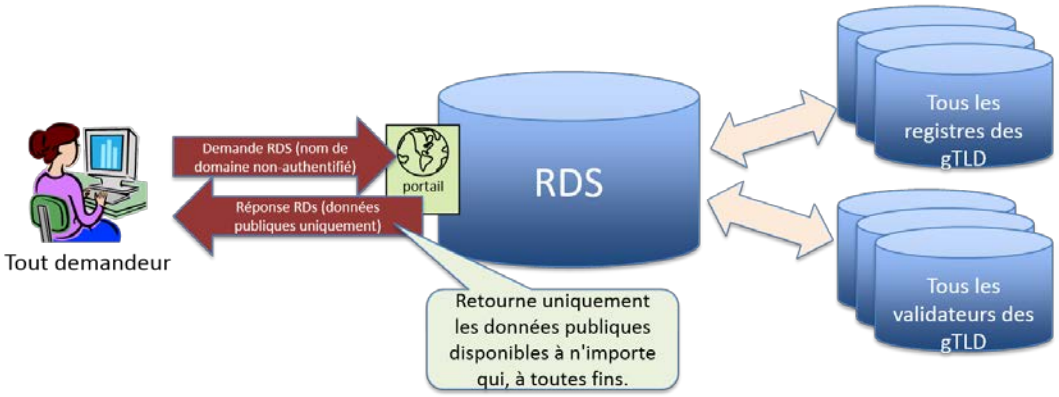
Un accès orienté sur les objectifs

Le RDS recommandé a pris une approche nouvelle, en abandonnant le système actuel unique WHOIS en faveur d'un accès à des données validées orienté sur les objectifs dans l'espoir d'améliorer la vie privée, l'exactitude et la responsabilité . L'EWG estime que cette nouvelle révolution conceptuelle de l'accès pourrait augmenter la responsabilité pour toutes les parties impliquées dans la divulgation et l'usage des données d'enregistrement des noms de domaine des gTLD par :

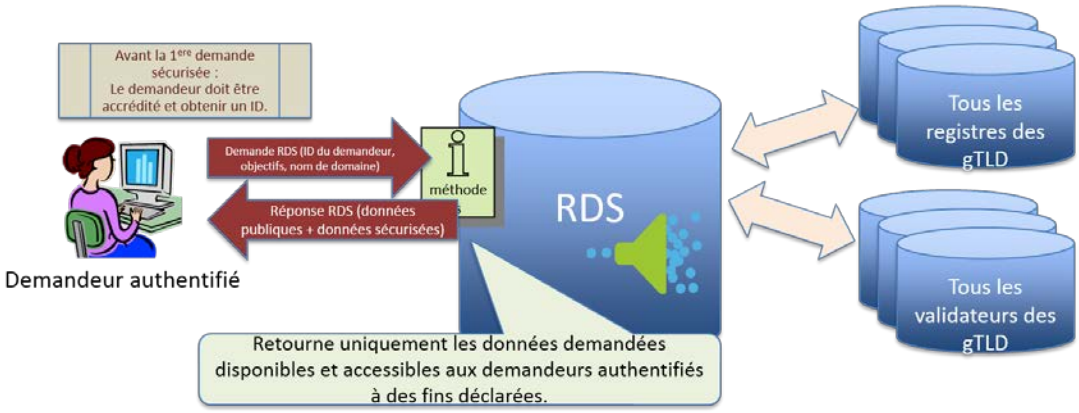
- la connexion de tous les accès aux données d'enregistrement des gTLD, y compris l'accès non-authentifié aux éléments de données publics, afin de permettre la détection et la réduction des abus ;
- le déclenchement d'un accès aux éléments de données les plus sensibles qui ne seraient disponibles que pour les personnes en faisant la demande et qui ont été accréditées pour recevoir un accès RDS, au niveau approprié pour chaque utilisateur et objectif énoncé et
- la vérification à la fois des accès aux données publiques et sécurisées afin de minimiser les abus et d'infliger des sanctions et autres recours pour usage

inapproprié, conformément aux conditions générales explicitement consenties par chaque demandeur.

Les principes de l'EWG pour les données d'accès qui ont servi de fondements pour ses recommandations détaillées sur l'accès aux données publiques et sécurisées, sont présentés en détail dans la section IV. Comme décrit ci-dessous, les éléments de données publics peuvent toujours être demandés à partir du RDS par n'importe qui, avec ou sans authentification.



Les éléments de données sécurisés peuvent également être demandés via le RDS. Pour ce faire, les requérants doivent d'abord être accrédités. Ensuite, les requérants peuvent soumettre leurs demandes authentifiées en demandant les éléments de données dans un objectif énoncé.



Se référer à l'annexe E pour une illustration plus détaillée des éléments de données retournés à la fois aux demandes de données publiques et sécurisées, de la manière dont l'accès sécurisé dépend de l'utilisateur et de l'objectif, et la manière dont les accréditeurs d'utilisateurs du RDS pourraient jouer un rôle dans l'autorisation et la vérification des accès sécurisés.

Confidentialité et protection des données

L'élément central du rôle de l'EWG concerne la question de la conception d'un système qui augmente l'exactitude des données collectées tout en offrant également les protections pour les titulaires cherchant à garder et maintenir leur vie privée.

L'EWG reconnait que les informations personnelles sont protégées par les lois relatives à la protection de la vie privée, et que même lorsqu'il n'y a pas de loi, il y a des raisons légitimes pour les individus de chercher une plus grande protection de leurs informations personnelles. De plus, les entreprises et les organisations peuvent chercher une protection de leurs informations à des fins légitimes, comme lorsqu'elles sont en train de préparer le lancement d'une nouvelle ligne de produits, ou, dans les cas de petites entreprises, lorsque les coordonnées divulguent des données personnelles.

En conséquence, l'EWG a formulé un ensemble de recommandations pour permettre de se conformer aux lois relatives à la protection des données et à la vie privée, détaillé dans la section VI. Ces principes englobent :

- des mécanismes pour faciliter la collecte de données conforme d'un point de vue juridique et le transfert entre les acteurs au sein de l'écosystème RDS ;
- des clauses de contrat standards qui sont harmonisées avec les lois relatives à la protection des données et de la vie privée et codifiées sur le plan politique ;
- un « moteur de règles » pour appliquer les lois relatives à la protection des données ; et
- la manière dont l'emplacement de stockage des données RDS est lié aux accès d'application de la loi.

En plus du respect de la vie privée garanti par la conformité aux lois de protection des données, le RDS a également recommandé des principes pour s'adapter aux besoins concernant la vie privée en incluant au sein de l'écosystème RDS :

- un service d'intermédiation ou d'anonymisation accrédité pour un usage général et
- un service de protection d'accès aux informations par identifiants sécurisés accrédité pour les personnes à risque et dans le cas où les droits à la liberté de parole ne seraient pas respectés ou les orateurs persécutés.

L'EWG a recommandé de manière plus approfondie que l'ICANN enquête sur le développement d'une seule politique de confidentialité harmonisée qui gouverne les activités du RDS de manière complète.

Pour répondre aux besoins concernant des services de protection d'accès aux informations par identifiants sécurisés plus fiables et uniformes qui permettent une

meilleure responsabilité, l'EWG a incorporé une partie sur la communication relative aux services d'intermédiation et d'anonymisation au sein de ses principes relatifs aux PBC. Il a également recommandé des principes relatifs aux services d'intermédiation et d'anonymisation et un cadre de contribution au groupe de travail de la GNSO sur les questions relatives aux services d'intermédiation et d'anonymisation.

Pour répondre aux besoins des particuliers et des groupes qui peuvent démontrer qu'ils pourraient encourir des risques s'ils étaient identifiés dans les données d'enregistrement, l'EWG préconise un cadre sécurisé par identifiant par lequel ces parties pourraient faire une demande anonyme et recevoir des noms de domaine enregistrés en utilisant des identifiants sécurisés, aidées par des validateurs et des tierces parties de confiance afin de fournir une protection entre les entités menacées et les bureaux d'enregistrement. L'EWG recommande que l'ICANN facilite l'établissement d'un conseil de révision de confiance et indépendant qui validera les réclamations concernant les organisations à risque ou les particuliers afin d'approuver (et révoquer si nécessaire) les identifiants.

Qualité des données

L'EWG recommande une validation plus solide des données des titulaires que celle fournie dans le système actuel WHOIS ou des améliorations qui peuvent être réalisées à travers une vaste mise en œuvre du 2013 RAA. Améliorations de base vers une qualité de données qui incluent ce qui suit.

- La mise à disposition des contacts orientés sur les objectifs par les titulaires devrait mener à des améliorations significatives pour l'accessibilité à des contacts appropriés à des fins diverses et apporte une motivation pour les titulaires de noms de domaine quant au fait de fournir des informations précises pour ces rôles.
- Avec un accès sécurisé à des éléments de données plus sensibles, les titulaires de noms de domaine seront moins encouragés à fournir des données inexactes, associés avec plus de responsabilité pour assurer l'exactitude des données.

De plus, l'EWG recommande deux améliorations indépendantes mais liées :

- Validation standard de toutes les données d'enregistrement des gTLD, en utilisant à la fois des vérifications périodiques et une validation au moment de la collecte, avec une possibilité de pré-valider des blocs de données de contact pour être réutilisés lors de multiples enregistrements de noms de domaine, ainsi que la capacité pour les utilisateurs du RDS de voir à quel moment les données ont été validées pour la dernière fois et à quel niveau ; et

- Un annuaire de contacts pré-validé, séparé sur le plan conceptuel de l'annuaire des noms de domaine, afin de promouvoir la qualité et l'utilité nouvelle des éléments de données utilisés pour contacter les titulaires de noms de domaine et les personnes ou les organisations qui peuvent être désignées par les titulaires des noms de domaine comme des PBC à diverses fins associés à l'enregistrement d'un nom de domaine, et afin de prévenir les usages frauduleux des données personnelles.

Les principes et les processus détaillant ces recommandations peuvent être trouvés dans la section V.

Modèles de mise en œuvre

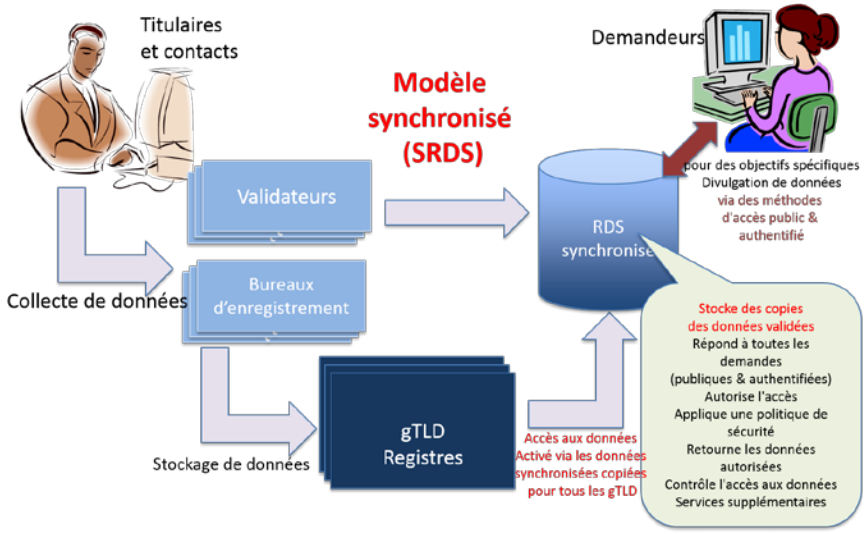
En prenant en considération la manière de mettre ces principes et recommandations en pratique, l'EWG a exploré plusieurs modèles d'alternatives en profondeur. Tous les modèles ont été évalués en utilisant des critères pluriels tels qu'identifiés à l'annexe F. Suite à une analyse rigoureuse, l'EWG a conclu ce qui suit.

- Aujourd'hui, les bureaux d'enregistrement ou les affiliés des bureaux d'enregistrement collectent et stockent des informations d'enregistrement pour leurs propres clients (les titulaires des noms de domaine). Ce processus est distribué de manière intrinsèque. En plus de continuer à collecter des données d'enregistrement des titulaires par les bureaux d'enregistrement ou leurs affiliés, l'EWG propose la collecte de données de contact par les validateurs.
- De multiples modèles possibles existent pour le stockage des informations d'enregistrement à travers tous les gTLD. L'EWG a identifié plusieurs modèles possibles et a localisé deux d'entre eux qu'il a jugé être les plus prometteurs, et il recommande que l'un d'eux soit choisi en utilisant des critères d'évaluation.
- Afin de protéger le caractère privé des données, une interface centralisée doit permettre aux demandeurs appropriés d'avoir accès aux informations d'enregistrement à travers tous les gTLD, y compris un accès non-authentifié aux données publiques et un accès authentifié aux données sécurisées.
- Le RDS doit utiliser le RDAP ou le protocole EPP (tel qu'approprié pour chaque interface) comme protocole d'accès aux annuaires sous-jacent afin d'obtenir des informations d'enregistrement à partir des emplacements de stockage, où qu'ils soient.

L'EWG a développé et testé plusieurs modèles de systèmes alternatifs, détaillés à l'annexe F, y compris des modèles suggérés par la communauté de l'ICANN. Ces modèles possibles diffèrent dans le sens où les informations d'enregistrement sont copiées ou demandées via le RDS. L'EWG a examiné de près chaque modèle afin de déterminer

l'impact de ces différences. Après la comparaison de ces modèles possibles, l'EWG a trouvé que, sauf pour l'actuel WHOIS, ils sont tous capables de satisfaire dans une certaine mesure les principes RDS recommandés par l'EWG. Parmi ceux-ci, l'EWG s'est concentré sur les deux modèles les plus prometteurs pour un examen plus approfondi, le modèle fédéré et le modèle synchronisé (anciennement connus sous le nom de « modèle intégré »).

Pour mieux valider leurs analyses, l'EWG a commandé une analyse relative au coût de mise en œuvre du modèle conduite par une tierce partie neutre (IBM) afin de déterminer les exigences et les éventuels coûts de ces deux modèles. Basé sur l'analyse en profondeur de l'EWG, ainsi que sur le rapport d'analyse d'IBM, qui a trouvé que le modèle fédéré serait plus couteux à l'écosystème RDS entier, **l'EWG a finalement recommandé le RDS synchronisé (SRDS).**



Conclusion

En raison des nombreux détails, de la complexité et de la longueur du rapport final, le présent rapport de synthèse ne donne pas un aperçu complet et nous encourageons les lecteurs à se référer au texte intégral du présent rapport final pour obtenir des informations supplémentaires .

L'EWG a remis le rapport final au président-directeur général de l'ICANN et au Conseil d'administration, l'a mis en ligne, et a mené de multiples consultations publiques lors de la réunion de l'ICANN de juin 2014 à Londres. Il conduira également des webinaires ainsi que d'autres occasions de discuter du rapport et de répondre aux questions à propos de celui-ci avec la communauté de l'ICANN. Le présent rapport final est destiné à servir de fondement pour le processus de développement de politiques de la GNSO demandé par

le Conseil pour les dispositions des données d'enregistrement des gTLD et pour des négociations contractuelles, selon le cas.

L'EWG est certain que le présent rapport final répond aux directives du Conseil d'administration de l'ICANN pour aider à redéfinir l'objectif et les dispositions en matière de données d'enregistrement des gTLD et fournira une base solide pour aider la communauté de l'ICANN (à travers l'organisation de soutien des noms génériques, GNSO) à créer une nouvelle politique mondiale pour les services d'annuaire gTLD.

II. Mandat, objectif et résultats de l'EWG

a. Mandat

Le groupe de travail d'experts du service d'annuaire d'enregistrement des gTLD (EWG) a été établi par le président-directeur général de l'ICANN, Fadi Chehadé, à la demande du Conseil d'administration de l'ICANN, dans le but d'aider à résoudre au sein de la communauté de l'ICANN l'impasse de près de dix ans sur la manière de remplacer le système WHOIS actuel. Plusieurs rapports de la communauté et études[4] publiés durant cette période identifient des faiblesses dans le système actuel lesquelles nécessitent une solution.

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 les besoins de la communauté Internet mondiale. Le groupe a commencé par faire table rase, explorant et remettant en question les hypothèses fondamentales à propos des objectifs, des utilisations, de la collecte, de l'entretien et de la mise à disposition des données d'enregistrement. L'EWG a pris en considération chaque partie prenante impliquée dans les services d'annuaire des gTLD, examinant leurs besoins en exactitude, accès et vie privée ainsi que des approches possibles pour répondre à ces besoins de manière plus efficace.

b. Objectif

Pour guider l'EWG dans ses délibérations, le groupe a élaboré une déclaration d'intention de haut niveau à partir de laquelle le groupe pourra vérifier ses conclusions et ses recommandations comme suit :

> Dans le but de soutenir la mission de l'ICANN pour coordonner le système d'identifiants uniques du système mondial de l'Internet et pour assurer l'opération stable et sécurisée du système d'identifiants 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

[44] Se référer à l'annexe B pour une liste des rapports qui présentent les faiblesses du WHOIS.

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 confidentialité des informations personnelles
- permettre un mécanisme fiable pour identifier, établir et maintenir la capacité à contacter des titulaires de noms de domaine ;
- soutenir un cadre pour aborder les questions qui impliquent les titulaires de nom de domaine, 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 de respect de la loi.

c. Résultats

Le 24 juin 2013, l'EWG a publié son rapport initial, une foire aux questions, et un questionnaire en ligne, et a lancé un processus de consultation approfondie au sein de la communauté de l'ICANN concernant ses recommandations initiales. Dans son rapport initial, l'EWG a conclu que le modèle actuel du WHOIS - qui donne à chaque utilisateur un même accès public anonyme à des données d'enregistrement de gTLD (souvent inexactes) devrait être abandonné. Au lieu du Whois, l'EWG recommandait un changement de paradigme selon lequel les données d'enregistrement de gTLD 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 est parvenu à cette recommandation après avoir dûment considéré des rapports précédents qui détaillaient les faiblesses du WHOIS et pris en considération les nombreuses parties prenantes différentes qui utilisent le système WHOIS actuel. Pour chaque groupe d'utilisateurs identifié, l'EWG a analysé les objectifs devant être satisfaits par les données d'enregistrement et les éléments de données individuels nécessaire pour ce faire. A la lumière de cette analyse, l'EWG a recommandé des principes et des caractéristiques afin de guider la création d'un service d'annuaire d'enregistrement de nouvelle génération (RDS). Afin d'illustrer le mode de mise en œuvre de ces principes, l'EWG a aussi examiné plusieurs alternatives et proposé un modèle pour la collecte et la divulgation d'éléments de données d'enregistrement de nom de domaine exacts à des fins autorisées.

Le 11 novembre 2013, après avoir soigneusement examiné tous les commentaires et remarques reçus de la part de la communauté de l'ICANN, l'EWG a publié un rapport de suivi, mettant en relief les réflexions de l'EWG sur plusieurs questions clés. Le rapport de suivi fournissait également beaucoup plus de détails sur l'analyse qui a abouti au rapport initial, tel que demandé par la communauté.

L'EWG a aussi procédé à une analyse détaillée des remarques reçues à propos de ces rapports, tirant parti des contributions diverses et approfondies de la communauté afin d'éclairer son travail en cours sur des points ouverts, de tester et d'affiner ses recommandations. Compte tenu de la complexité de la tâche à accomplir et de l'importance de l'établissement d'un RDS de nouvelle génération sur une compréhension solide des avantages et des impacts éventuels, l'EWG a mené une recherche dans cinq domaines : les pratiques existantes de validation de données commerciales et des ccTLD, les pratiques existantes de fournisseurs de service d'intermédiation / d'anonymisation, l'examen d'organisations en mesure d'accréditer les utilisateurs du RDS et l'analyse des risques/bénéfices et coûts du RDS. Les résultats de cette recherche, publiée en mars 2014, ont été utilisés pour affiner les recommandations de l'EWG.

A ce stade, l'EWG a soigneusement considéré le travail déjà accompli sur le WHOIS, les utilisateurs existants et éventuels futurs des données d'enregistrement de gTLD et leurs objectifs, les contributions des nombreuses parties prenantes diverses dans le système actuel du WHOIS, les pratiques existantes associées aux améliorations du RDS proposées et l'analyse des risques, bénéfices et coûts du RDS. Toutes ces contributions ont éclairé les les recommandations de l'EWG[5] pour un système de nouvelle génération

[5] Tout au long de ce rapport, les principes de l'EWG utilisent les termes suivants, basés sur les définitions données dans la RFC 2119:

- DOIT : Ce mot, ou les termes « REQUIS » ou « DEVRA » signifie que la définition est une nécessité absolue de ce rapport.
- NE DOIT PAS : Cette phrase, ou la phrase « NE DEVRA PAS » signifie que la définition est une interdiction absolue de ce rapport.
- DEVRAIT : Ce mot, ou l'adjectif « RECOMMANDÉ » signifie qu'il peut exister des raisons valables dans des circonstances particulières pour ignorer un point particulier, mais que toutes les conséquences doivent être comprises et soigneusement considérées avant de choisir une voie différente.
- NE DEVRAIT PAS : Cette phrase, ou la phrase « NON RECOMMANDÉ » signifie qu'il peut exister des raisons valables dans des circonstances particulières où le comportement particulier est

décrit en détail dans ce rapport final au Conseil d'administration de l'ICANN visant à servir de contribution ciblée pour le processus de développement de politique.

acceptable ou même utile, mais que toutes les conséquences devraient être comprises et le cas soigneusement considéré avant de mettre en œuvre un comportement décrit comme non recommandé.

III. Utilisateurs et objectifs

a. Méthodologie

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, plutôt que d'améliorer le système Whois actuel, qui est largement perçu comme inapproprié. 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 une grande variété d'utilisateurs.

Pour y parvenir, les membres de l'EWG ont travaillé sur un vaste 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 mise à disposition 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 utilisateurs et leurs besoins 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 à l'annexe C.

L'EWG a analysé tous ces cas d'utilisation et en a tiré des leçons afin d'identifier un ensemble consolidé de parties prenantes et d'objectifs souhaitables qui devraient être desservis par le RDS, ainsi qu'un ensemble d'utilisations abusives potentielles que le système devrait être en mesure de prévenir (voir 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.

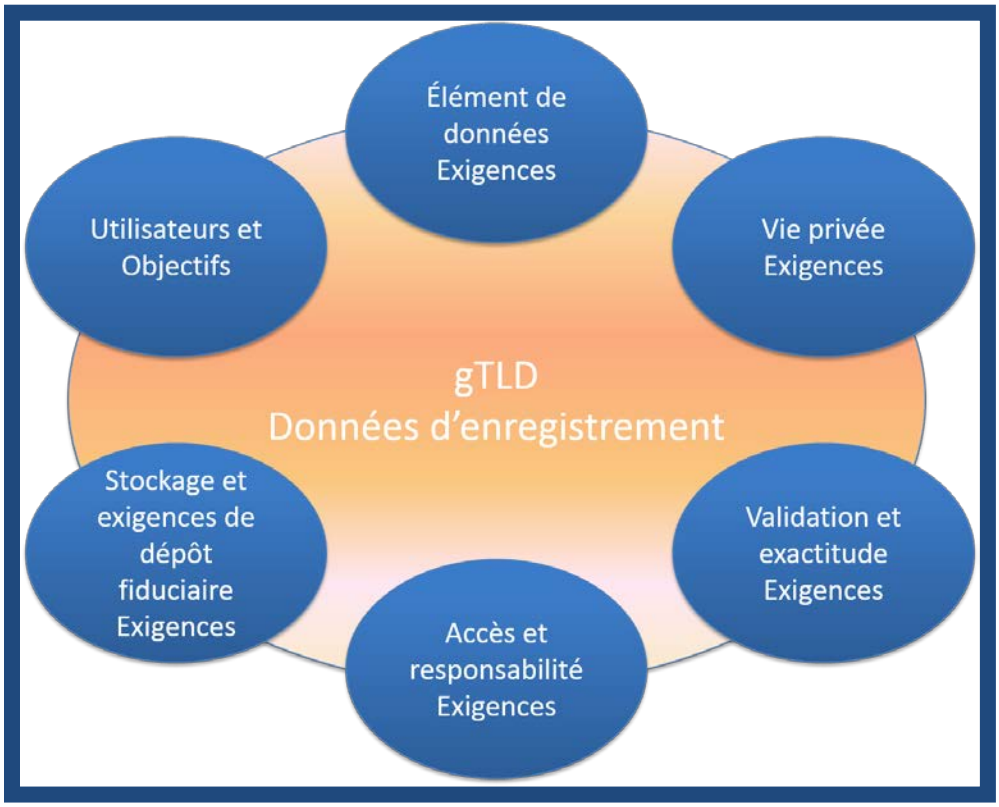


Figure 1 : Besoins d'analyse

L'EWG a poursuivi son travail en analysant ces objectifs et besoins d'utilisateurs afin d'identifier un ensemble minimum d'éléments de données nécessaire pour chaque objectif, les risques associés à la mise à disposition de ces données, les implications en matière de loi et de politique relatives à la vie privée et d'autres questions examinées dans ce rapport.

b. Utilisateurs du RDS et objectifs

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

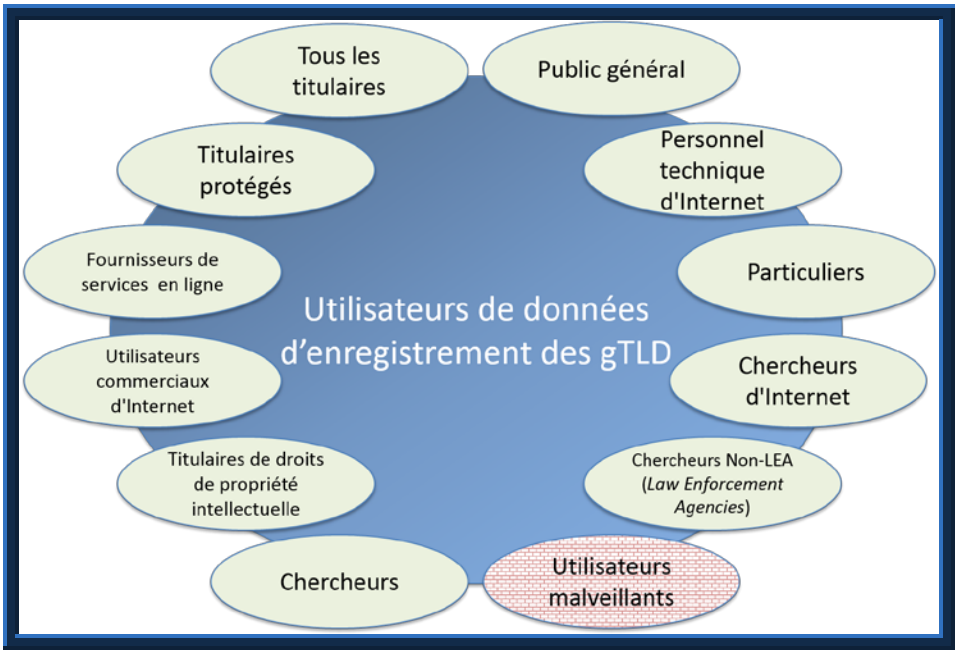


Figure 2 : Utilisateurs

Dans ce rapport, le terme « demandeur » est utilisé pour décrire génériquement tous les utilisateurs qui souhaitent obtenir les données d'enregistrement gTLD du système. Tel qu'il est détaillé dans ce rapport, l'EWG recommande d'abandonner le modèle du WHOIS actuel qui donne à tous les utilisateurs le même accès public anonyme à des données d'enregistrement gTLD (trop souvent inexactes). 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 a analysé 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. De plus amples détails sur chaque utilisateur, objectif et sur les besoins en données y associés sont fournis dans la section III(c), les objectifs à desservir ou à interdire et à l'annexe D.

Utilisateur	But	Exemples de cas d'utilisation	Fondements pour l'enregistrement des données d'accès
Tous les titulaires (par ex., personnes physiques, personnes	Contrôle du nom de domaine	Création d'un compte pour l'enregistrement de noms de	Permettre l'enregistrement de noms de domaine par tout titulaire de nom de domaine que crée un

Utilisateur	But	Exemples de cas d'utilisation	Fondements pour l'enregistrement des données d'accès
morales, fournisseurs des services d'intermédiation/d'anonymisation)		domaine	nouveau compte auprès d'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, actuelle ou passée (utilisant WhoWas)
		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
		Démarrage de transfert de nom de domaine	Permettre le transfert d'un nom de domaine initié par un titulaire de nom de domaine 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 titulaire de nom de domaine
		Renouvellement des noms de domaine	Permettre le renouvellement d'un nom de domaine enregistré par le titulaire du nom de domaine
		Validation du contact du nom de domaine	Faciliter la validation initiale et continue des données d'enregistrement (par ex., contacts désignés, adresses) par le titulaire du nom de domaine
Titulaires protégés (par ex. clients de fournisseurs accrédités de services d'intermédiation/d'anonymis	Protection des données personnelles	Contact fournisseur de services d'intermédiation /	Permettre le contact avec des fournisseurs de services d'intermédiation/d'anonymisation accrédités utilisés par tout titulaire de nom de domaine cherchant à

Utilisateur	But	Exemples de cas d'utilisation	Fondements pour l'enregistrement des données d'accès
ation qui doivent être contactés)		d'anonymisation	minimiser l'accès public aux données et aux adresses personnelles.
		Contact approbateur identifiant sécurisé	Permettre le contact avec des approbateurs d'identifiants sécurisés accrédités offrant des services d'enregistrement utilisés par des individus ou des groupes menacés, utilisation des identifiants sécurisés relayés via tierce partie fiable
Personnel technique d'Internet (par ex., administrateurs du DNS, administrateurs du courriel, administrateurs Web, FSI)	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)
Autorités de certification	Certification des noms de domaine	Émission de certification des noms de domaine	Aider une autorité de certification (CA) à identifier le titulaire d'un nom de domaine lié à un certificat SSL/TLS
Internautes particuliers (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 titulaire de nom de domaine du nom de domaine (par ex. adresse commerciale)
		Protection du consommateur	Disposer d'un mécanisme simple pour que les consommateurs puissent contacter les contacts commerciaux des titulaires de noms de domaine (par ex., le service clientèle des détaillants en ligne) afin de résoudre les problèmes rapidement, sans

Utilisateur	But	Exemples de cas d'utilisation	Fondements pour l'enregistrement des données d'accès
			l'intervention de LE/OpSec.
Utilisateurs commerciaux d'Internet (par ex. détenteurs de marques, courtiers, agents)	Achat ou vente des noms de domaine commerciaux	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 titulaires de noms de domaine en appui à l'analyse des risques lors de l'établissement de nouvelles marques
		Acquisition de noms de domaine	Faciliter l'acquisition d'un nom de domaine enregistré au préalable en permettant le contact avec le titulaire de nom de domaine
		Demande d'achat d'un nom de domaine	Permettre de déterminer la disponibilité d'un nom de domaine et le titulaire et administrateur de nom de domaine actuels (le cas échéant)
		Historique d'enregistrement d'un nom de domaine	Fournir l'historique de l'enregistrement de noms de domaine pour identifier les anciens titulaires de noms de domaine et les dates en utilisant WhoWas
		Noms de domaine pour des titulaires de nom de domaine spécifiques	Permettre de déterminer tous les noms de domaine enregistrés par une entité spécifique (requête inverse) dans le cadre de la vérification des actifs en cas de fusion/création
Chercheurs d'Internet	Recherche du DNS académique/d'intérêt public	Historique d'enregistrement d'un nom de domaine	Permettre la recherche historique concernant l'enregistrement d'un nom de domaine (WhoWas) pendant une recherche du DNS académique/d'intérêt public
		Noms de domaine pour	Permettre l'identification de tous les noms de domaine

Utilisateur	But	Exemples de cas d'utilisation	Fondements pour l'enregistrement des données d'accès
		des contacts spécifiques	enregistrés avec un nom, une adresse, un nom de serveur, une date d'enregistrement, etc. donnés (requête inverse) pendant une recherche du DNS académique d'intérêt public
		Enquête sur les titulaires de noms de domaine ou contacts désignés	Permettre les enquêtes sur les titulaires de noms de domaine ou leurs contacts désignés
Titulaires de droits de propriété intellectuelle (par ex., propriétaires de marques commerciales, propriétaires de propriété intellectuelle)	Actions juridiques	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 PI
		Combattre l'utilisation frauduleuse des données d'enregistrement	Faciliter l'identification et répondre à l'utilisation frauduleuse de données légitimes (par ex., adresse) pour des noms de domaine appartenant à un autre titulaire de nom de domaine en utilisant la requête inverse sur les données d'identité validées
		Historique d'enregistrement d'un nom de domaine	Permettre la recherche historique concernant l'enregistrement d'un nom de domaine (WhoWas) pendant une recherche concernant une violation de PI
		Noms de domaine pour des titulaires de nom de domaine spécifiques	Permettre l'identification de tous les noms de domaine enregistrés avec un nom ou une adresse donnés (requête inverse) durant une recherche concernant une violation de PI

Utilisateur	But	Exemples de cas d'utilisation	Fondements pour l'enregistrement des données d'accès
Enquêteurs Non-LEA (*Law Enforcement Agencies*) (par ex., autorités fiscales, fournisseurs UDRP, conformité de l'ICANN)	Exécution des contrats/règlementation	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	Permettre aux fournisseurs UDRP de confirmer l'identité du responsable correct d'un nom de domaine, de réaliser des vérifications de la conformité, de déterminer les exigences des procédures judiciaires et de protéger contre le « cyberflight »
		Conformité contractuelle de l'écosystème du RDS	Permettre à l'ICANN de réaliser des audits et de répondre aux plaintes concernant la non conformité de la part des parties contractantes (par ex., inexactitude ou non-disponibilité des données, décision de mise en œuvre de l'UDRP, plaintes de transfert, rétention et dépôt de données)
Enquêteurs LEA/OpSec (par ex., organismes d'application de la loi, équipes de réponse aux incidents)	Enquête policière & réduction des abus de DNS	Examiner les noms de domaine abusifs	Permettre l'analyse efficace et la collecte de preuves par le personnel des LEA/OpSec en réponse à l'enregistrement supposé malveillant d'un nom de domaine, y compris l'examen de données historiques
		Enquêter sur l'activité criminelle hors ligne	Permettre l'enquête efficace et la collecte de preuves par le personnel des LEA/OpSec en réponse à une activité criminelle hors ligne en fournissant des données d'enregistrement détaillées et/ou en recherchant des noms de domaine enregistrés par le suspect (requête inverse)

Utilisateur	But	Exemples de cas d'utilisation	Fondements pour l'enregistrement des données d'accès
		Services de réputation en matière de noms de domaine	Permettre l'analyse des listes noire/blanche des noms de domaine par des fournisseurs de services de réputation
		Enquêter sur l'activité criminelle en ligne	Aider les victimes ou leurs avocats-conseils à identifier le titulaire du nom de domaine impliqué dans des activités illégales potentielles pour permettre une enquête ultérieure des LE/OpSec.
		Point de contact pour les abus des noms de domaine compromis	Assister à rétablir des noms de domaine compromis en aidant le personnel des LEA/OpSec à contacter le titulaire du nom de domaine ou le responsable des abus désigné
Public général (par ex. blogueurs, médias, activistes politiques)	Transparence du DNS	Accès aux données d'enregistrement publiques	Identifier l'organisation « derrière » un nom de domaine, tel que généralement souhaité par une grande variété d'internautes non autrement reflétés dans des cas d'utilisation plus spécifiques
Utilisateurs malveillants (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 titulaire de nom de domaine et détourner le/s nom/s de domaine de ce titulaire de nom de domaine
		Enregistrement malveillant d'un nom de domaine	Utiliser un compte d'enregistrement d'un nom de domaine existant/compromis pour enregistrer de nouveaux noms en appui à des activités criminelles, frauduleuses ou abusives
		Fouille des	Obtenir les données

Utilisateur	But	Exemples de cas d'utilisation	Fondements pour l'enregistrement des données d'accès
		données d'enregistrement pour Pourriel/Escroquerie	d'enregistrement d'un nom de domaine pour son utilisation malveillante par des spammeurs, des escrocs et d'autres criminels (malveillants)

Tableau 1. Utilisateurs du RDS et objectifs

c. Objectifs à desservir ou à interdire

L'EWG a cherché à donner la priorité aux objectifs énumérés ci-dessus pour se concentrer sur le développement des cas d'utilisation et rétrécir l'éventail des objectifs admissibles. Toutefois, il a été difficile d'établir les fondements pour répondre aux besoins de quelques utilisateurs qui utilisent aujourd'hui le système actuel du Whois mais pas d'autres, tant que leurs fins ne soient pas illicites. Ce résultat a amené l'EWG à recommander que toutes les fins admissibles identifiées devraient être desservies par le RDS en quelque sorte, exception faite des activités illicites connues sur Internet qui devraient être activement découragées. les objectifs admissibles recommandés par l'EWG sont résumés ci-dessous.

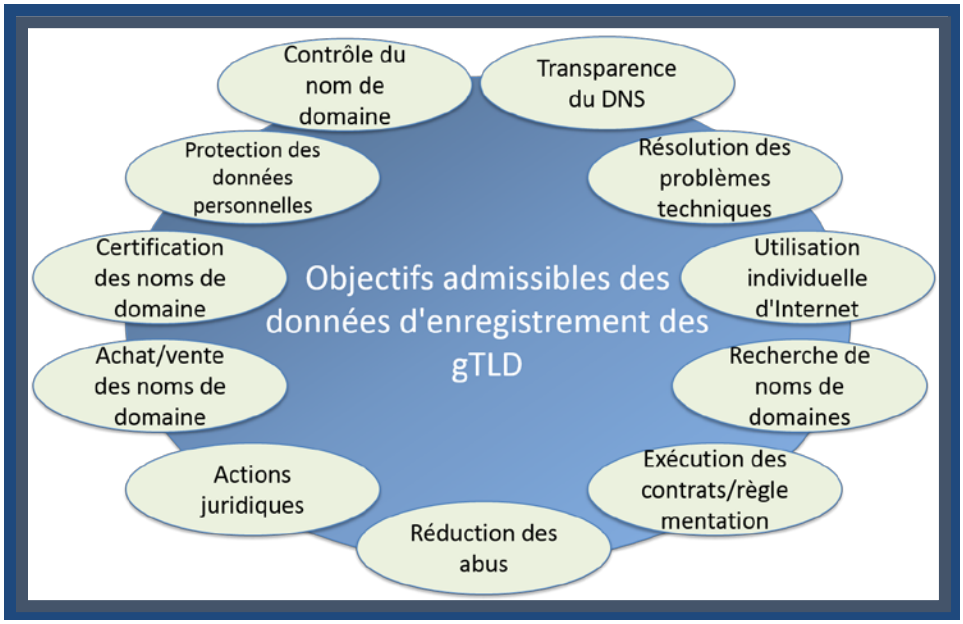


Figure 3 : Objectifs admissibles

Il faudrait noter que dans chaque objectif, il y a un très grand nombre de cas d'utilisation existants et éventuels futurs. Bien que l'EWG n'ait pas tenté d'identifier tous les cas d'utilisation possibles, il s'est efforcé d'explorer un échantillon représentatif

dans l'espoir de rigoureusement identifier les types d'utilisateurs, ainsi que leurs fins ou objectifs lorsqu'ils veulent accéder à des données d'enregistrement gTLD. Toutefois, le RDS doit être conçu avec la capacité d'accueillir de nouveaux utilisateurs et objectifs admissibles qui pourraient apparaître au fil du temps.

L'analyse des cas d'utilisation énumérés à l'annexe C faite par l'EWG, a mis en évidence qu'un bon nombre d'utilisateurs avaient 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
- La capacité de contacter quelqu'un à propos du nom de domaine

Toutefois, certains besoins sont communs et pourtant ne sont pas satisfaits par le système Whois en vigueur de manière conséquente. En voici quelques exemples :

- la capacité de déterminer tous les domaines enregistrés par une entité donnée (généralement mentionnée comme WHOIS inverse)
- La capacité de déterminer des informations historiques concernant l'enregistrement d'un nom de domaine (généralement mentionnée comme WhoWas)

L'EWG a pris ces besoins communs en considération lors de l'élaboration des recommandations du RDS détaillées dans le présent rapport. Toutefois, comme il est probable que les futurs besoins communs seront identifiés au fil du temps, le système de nouvelle génération doit être conçu en ayant à l'esprit son extensibilité. les objectifs admissibles actuellement identifiés par l'EWG et les données d'enregistrement, les contacts et les besoins de requête y associés sont définis ci-dessus.

Objectif	Définition
Contrôle du nom de domaine	Les tâches propres au champ de cet objectif incluent : créer, gérer et surveiller un nom de domaine propre à un titulaire (DN), y compris la création du nom de domaine, la mise à jour d'informations à propos du nom de domaine, le transfert du nom de domaine, le renouvellement du nom de domaine, la suppression du nom de domaine, le maintien d'un portefeuille de nom de domaine, et la détection d'usage frauduleux des informations de contact propre au titulaire. Ceci implique que chaque titulaire de nom de domaine doit être un utilisateur authentifié du RDS pour cet objectif, avec la capacité d'accéder à toutes les informations publiques et sécurisées dans le RDS concernant leur nom de domaine, y compris les données du contact désigné publiées dans le RDS pour ce nom de domaine.

Objectif	Définition
Protection des données personnelles	Les tâches propres au champ de cet objectif incluent : identifier le fournisseur de services d'intermédiation/d'anonymisation accrédité associé avec le nom de domaine et signalant l'abus, demandant la divulgation ou autrement contacter le fournisseur. Pour accomplir ces tâches, l'utilisateur a besoin de contacter le fournisseur de services d'intermédiation / d'anonymisation facilement et de manière fiable - par exemple en suivant l'URL du contact du fournisseur de services d'intermédiation/d'anonymisation en cas d'abus pour parvenir à une page qui décrit le processus de divulgation du fournisseur ou permet à l'utilisateur de soumettre un formulaire de demande de divulgation.
Résolution des problèmes techniques	Les tâches propres au champ de cet objectif incluent : travailler sur la résolution de problèmes techniques liés à l'utilisation de noms de domaine, y compris les questions de transmission de courriels, les problèmes de résolution du DNS et les problèmes fonctionnels des sites Web. Pour accomplir ces tâches, l'utilisation a besoin de la capacité de contacter le responsable du personnel technique afin de traiter ces problèmes. (Remarque : il pourrait être utile de désigner de multiples points de contact afin d'aborder les divers types de problèmes - par exemple, un postmaster pour les questions de courriel).
Certification des noms de domaine	Les tâches propres au champ de cet objectif incluent une autorité de certification (CA) qui délivre un certificat X.509 à un sujet identifié par un nom de domaine. Pour accomplir cette tâche, l'utilisateur a besoin de confirmer que le nom de domaine est enregistré au sujet du certificat ; pour ce faire, il est nécessaire d'accéder à toutes les données publiques et sécurisées relatives au titulaire du nom de domaine.
Utilisation individuelle d'Internet	Les tâches propres au champ de cet objectif incluent : identifier l'organisation utilisant un nom de domaine pour créer un climat de confiance avec le consommateur, ou contacter cette organisation pour lui porter une plainte d'un client ou déposer une plainte contre cette organisation. Pour accomplir ces tâches, l'utilisateur a besoin du nom de l'organisation (à identité validée de préférence) et de son adresse (postale) légale. Il serait utile de pouvoir suivre une URL de contact vers une page qui décrive l'organisation et ses contacts en matière de service clientèle ou de permettre à l'utilisateur de soumettre une demande de service client.

Objectif	Définition
Achat ou vente des noms de domaine commerciaux	Les tâches propres au champ de cet objectif incluent : réaliser des enquêtes d'achat à propos d'un nom de domaine, acquérir un nom de domaine d'un autre titulaire et permettre un processus de recherche raisonnable. Pour accomplir ces tâches, l'utilisateur a besoin d'accéder à l'organisation du titulaire du nom de domaine et à l'adresse électronique et dans certains cas à des données supplémentaires sécurisées - par ex. pour procéder à une requête inverse concernant le nom ou le contact d'un titulaire de nom de domaine pour déterminer s'il y a d'autres noms de domaine auxquels ils sont associés.
Recherche du DNS académique/d'intérêt public	Les tâches propres au champ de cet objectif incluent les études de recherche d'intérêt public et académique à propos des noms de domaine publiées dans le RDS, y compris des informations publiques concernant le titulaire et les contacts désignés, l'histoire et le statut du nom de domaine, et les noms de domaine enregistrés par un titulaire donné (requête inverse). Pour accomplir ces tâches, l'utilisateur a besoin d'accéder à toutes les données publiques dans le RDS et dans certains cas, il pourrait avoir besoin d'accéder à des données sécurisées pour utilisation sous forme résumée anonymisée.
Actions en justice	Les tâches propres au champ de cet objectif incluent : rechercher d'éventuels usages frauduleux de nom ou d'adresse d'un titulaire par d'autres noms de domaine, rechercher d'éventuelles atteintes aux marques déposées, contacter un représentant juridique du titulaire/détenteur de licence avant d'intenter des poursuites judiciaires et ensuite, intenter des poursuites judiciaires si le problème n'est pas résolu de manière satisfaisante. Pour accomplir ces tâches, l'utilisateur a besoin de pouvoir contacter le représentant légal du titulaire / détenteur de licence, sans passer par l'intermédiaire d'un fournisseur de services d'intermédiation/d'anonymisation accrédité.
Exécution des contrats/règlementation	Les tâches propres au champ de cet objectif incluent l'enquête commerciale des autorités fiscales avec une présence en-ligne, une enquête UDRP (politique uniforme de règlement de litiges relatifs aux noms de domaine), enquête de conformité contractuelle, et audit de dépôt fiduciaire des données d'enregistrement. Pour les accomplir, l'utilisateur accrédité a besoin d'accéder à quelques éléments sécurisés de données du nom de domaine et de contact du titulaire du nom de domaine, tels que l'adresse postale et le numéro de téléphone, selon le cas et l'objectif. Par exemple, l'OMPI pourrait avoir besoin d'accéder à une résolution d'UDRP.
Enquête policière & réduction des abus de DNS	Les tâches propres au champ de cet objectif incluent : rapporter les abus à une personne qui peut enquêter et traiter ces abus, ou contacter les entités associées à un nom de domaine pendant une enquête policière hors ligne. Pour accomplir ces tâches, l'utilisateur accrédité (par ex. l'agent responsable de la loi, le premier répondant) a besoin de contact rapidement et de manière

Objectif	Définition
	fiable le contact responsable en cas d'abus lié au nom de domaine - par exemple, en suivant une URL vers une description de la procédure de signalement d'abus ou le formulaire de signalement d'incident.
Transparence du DNS	Les tâches propres au champ de cet objectif impliquent la recherche des données d'enregistrement rendues publiques par les titulaires de noms de domaine afin de satisfaire une grande variété de cas d'utilisation autour de l'information du grand public. Pour accomplir ces tâches, l'utilisateur a besoin d'accéder facilement aux données publiques (et uniquement à ces données) qui peuvent être fournies par le RDS. Les titulaires de noms de domaine doivent être informés que les données publiques d'enregistrement de leurs noms de domaine peuvent être utilisées dans le cadre de cet objectif « passe-partout », et cet objectif doit être limité aux données publiques (c'est-à-dire que cet objectif ne permet PAS l'accès à des données sécurisées).

Tableau 2. Définitions des objectifs

Le champ de données d'enregistrement nécessaires pour satisfaire ces objectifs est résumé dans le tableau ci-dessous, y compris les noms de domaine impliqués, les types de données nécessaires (données du titulaire, coordonnées de contact, données du nom de domaine) ainsi que les requêtes supplémentaires nécessaires.

Objectif	Champ de requête	Contact(s) nécessaires	Données du du titulaire nécessaires	Données du ND	Autres requêtes nécessaires
Contrôle du nom de domaine	Propre ND	Tous	Publiques et sécurisées	Oui	Inverse (propres données) WhoWas (propre nom de domaine)
Protection des données personnelles	ND PP*	PP	Publiques	Oui	Aucune
Résolution des problèmes techniques	Tout ND	Technique	Publiques	Oui	Aucune
Certification des noms de domaine	Tout ND	Aucun	Publiques et sécurisées	Oui	Aucune
Utilisation individuelle d'Internet	ND LP*	Commercial	Publiques	Non	Aucune
Achat/vente des noms de domaine commerciaux	Tout ND	Admin.	Publiques Approuvées Sécurisées	Oui	Inverse (données approuvées) WhoWas (tout nom de domaine)
Recherche du DNS académique/d'intérêt public	Tout ND	Tous	Publiques et Approuvées Sécurisées	Oui	Inverse (données approuvées) WhoWas (tout nom de domaine)
Actions juridiques	Tout ND	Juridique	Publiques et Approuvées	Oui	Inverse (données approuvées)

			Sécurisées		WhoWas (tout nom de domaine)
Exécution des contrats/règlementation	Tout ND	Juridique	Publiques et sécurisées	Oui	Inverse (toutes données) WhoWas (tout nom de domaine)
Enquête policière & réduction des abus de DNS	Tout ND	Abus	Publiques et sécurisées	Oui	Inverse (toutes données) WhoWas (tout nom de domaine)
Transparence du DNS	Tout ND		Publiques	Oui	Aucune

Tableau 3. Champ de données d'enregistrement nécessaires pour chaque objectif

Au tableau 3, « les données sécurisées approuvées » pourraient être définies par des conditions de service que les utilisateurs du RDS accrédités peuvent demander, sous réserve to politiques définies qui couvrent :

- qui est habilité à un accès sécurisé
- la motivation légitime du besoin de ces données
- les restrictions s'appliquant à l'usage de ces données
- la supervision requise pour garantir l'usage approprié

Ces objectifs ayant besoin de « données sécurisées approuvées » nécessitent une analyse plus approfondie, en consultation avec ces communautés d'utilisateurs du RDS, pour déterminer comment de telles politiques pourraient être raisonnablement définies, appliquées et mises en vigueur, en équilibre avec les besoins de responsabilité et de confidentialité. Toutefois, les exemples suivants sont donnés afin d'illustrer le mode de fonctionnement éventuel :

- **La recherche du DNS académique/d'intérêt public** pourrait impliquer un chercheur d'une université reconnue, engagé dans une étude spécifique du DNS, ayant énuméré les éléments de données sécurisés requis et comment ils seront utilisés, d'accord pour publier les résultats seulement sous une forme globale/anonymisée, sous réserve d'une supervision d'un conseil de révision indépendant (IRB). Sa « recherche du DNS d'intérêt public » ayant été approuvée, l'utilisateur du RDS accrédité pourrait avoir le droit d'accéder à certains éléments de données sécurisés du titulaire de nom de domaine ou demander ces éléments de données dans une requête inverse.
- Une enquête sur **l'achat/la vente d'un ND** pourrait impliquer un utilisateur commercial, engagé dans une transaction commercial nécessitant un contrôle préalable concernant les actifs du nom de domaine détenu par un vendeur. Par un suivi et une supervision de la part d'une entité d'accréditation (définie à la section IV(c), accréditation de l'utilisateur du RDS), cet utilisateur pourrait

attester que non seulement il est engagé dans l'achat d'un nom de domaine mais aussi que les données du RDS sont requises pour permettre un contrôle préalable à propos du vendeur « X » et que les résultats seront seulement utilisés pour cet objectif spécifique. Ayant reçu l'approbation pour utiliser le DNS afin d'effectuer ce type de vérification préalable, l'utilisateur accrédité du RD peut avoir le droit d'utiliser des requêtes inverses afin de rechercher des noms de domaine avec des données sécurisées approuvées associées au vendeur « X », tel que détaillé à l'annexe E.

- L'enquête pour une **action en justice** peut impliquer un avocat habilité à enquêter dans des cas de violation de marques déposées. Par un suivi et une supervision de la part d'une entité d'accréditation (définie à la section IV(c), accréditation de l'utilisateur du RDS), cet utilisateur pourrait attester que non seulement il est en train d'enquêter dans le cadre d'une action juridique éventuelle, mais aussi que les données du RDS sont requises pour permettre une enquête sur un sujet « Y » et que toutes données trouvées seront seulement utilisés pour cet objectif restreint. Ayant reçu l'approbation pour utiliser le DNS afin d'effectuer ce type d'enquête sur violation de marque déposée, l'utilisateur accrédité du RD peut avoir le droit d'utiliser des requêtes inverses afin de rechercher des noms de domaine avec des données sécurisées approuvées associées au sujet « Y », tel que détaillé à l'annexe E.

Pour illustrer les données impliquées dans ces objectifs, le rôle des données sécurisées approuvées et les protections qui pourraient être mises en place afin de tenir les utilisateurs responsables et décourager les abus, voir l'annexe E, Illustrations d'accès sécurisé et non authentifié.

Cette exploration des utilisateurs du RDS et des objectifs admissibles a conduit l'EWG à formuler les principes fondamentaux suivants afin de permettre un accès aux données d'enregistrement basé sur l'objectif :

Nº.	Principes des objectifs admissibles
1.	L'ICANN doit publier, en un endroit, une politique conviviale qui décrit l'objectif et les usages admissibles des données d'enregistrement, afin d'informer les titulaires de noms de domaine de manière claire pourquoi ces données sont recueillies et comment elles seront traitées et utilisées.
2.	Des utilisations admissibles /inadmissibles du RDS devraient être clairement définies.
3.	Le RDS doit soutenir les objectifs admissibles définis, y compris les utilisations qui impliquent :

	• identifier le titulaire du nom de domaine et les contacts désignés pour un objectif donné ; • communiquer avec les contacts désignés pour un objectif donné ; • utiliser les données publiées par les registres à propos des noms de domaine et • recherche des parties des données d'enregistrement requises pour un objectif donné.
4.	Le RDS doit être conçu avec la capacité d'accueillir de nouveaux utilisateurs et des objectifs admissibles qui pourraient apparaître au fil du temps. • Un processus de demande doit être défini. • Les demandes doivent être examinées en fonction des critères définis • Les demandes qui passent l'étape de révision doivent être évaluées et approuvées par un conseil de révision multipartite tel que défini par un processus de développement de politique • Les demandes approuvées doivent être ajoutées à la politique de confidentialité du RDS et programmées pour une mise en œuvre périodique (par ex. trimestrielle, annuelle) tel que défini par la politique Note : voir section VI éléments de données pour le processus d'ajout de nouveaux éléments de données.
5.	Tous les objectifs admissibles identifiés devraient être desservis par le RDS *en quelque sorte*, exception faite des activités illicites connues sur Internet qui devraient être activement découragées. les objectifs admissibles recommandés par l'EWG sont résumés au tableau 1, utilisateurs du RDS et objectifs et à la figure 3, objectifs admissibles.
6.	Les données d'enregistrement de gTLD devraient être recueillies, validées et divulguées seulement pour des objectifs admissibles, avec certains éléments de données accessibles seulement aux demandeurs authentifiés qui sont tenus responsables de l'usage approprié.
7.	Chaque titulaire de nom de domaine doit avoir la capacité d'accéder à toutes les informations publiques et sécurisées publiées dans le RDS concernant son nom de domaine, y compris les coordonnées des contacts désignés.

d. Parties prenantes impliquées dans le RDS

Le tableau suivant fournit un résumé représentatif des diverses parties prenantes impliquées dans la collecte, l'enregistrement, la divulgation et l'utilisation des données d'enregistrement des gTLD, appliquées aux objectifs associés Certaines parties prenantes fournissent des données (par ex., les titulaires de nom de domaine), alors que d'autres collectent/entreposent des données (par ex., les validateurs, les registres et les bureaux d'enregistrement) ou divulguent des données (par ex., l'opérateur RDS, les fournisseurs de services d'anonymisation/d'intermédiation). 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 touchées par les données divulguées (par ex., contacts en 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	Fins ou objectifs
Contact en cas d'abus des noms de domaine	Enquête policière & réduction des abus de DNS
Société acquérante	Achat ou vente des noms de domaine commerciaux
Agents/avocats de la société acquérante	Achat ou vente des noms de domaine commerciaux
Service de validation d'adresses	Contrôle du nom de domaine
Agents du titulaire de nom de domaine	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	Certification des noms de domaine
Plaignant	Exécution des contrats/règlementation
Consommateurs achetant des produits de sites Web	Utilisation individuelle d'Internet
Utilisateurs accédant à des sites Web	Utilisation individuelle d'Internet
Intermédiaire d'un domaine	Achat ou vente des noms de domaine commerciaux
Acheteur d'un domaine	Achat ou vente des noms de domaine commerciaux
Victime de fraude	Actions en justice
Agent de la victime de fraude	Actions en justice
Personnel de l'agence gouvernementale	Exécution des contrats/règlementation
Conformité de l'ICANN	Exécution des contrats/règlementation
Panel de révision indépendant (IRP)	Recherche du DNS académique/d'intérêt public
Fournisseurs de services Internet	Résolution de problèmes techniques Enquête policière et réduction des abus
Enquêteur	Utilisation individuelle d'Internet
Personnel des organismes d'application de la loi	Enquête policière & réduction des abus Poursuites juridiques
Contact du fournisseur de services d'anonymisation/d'intermédiation sur la liste	Protection des données personnelles Contrôle du nom de domaine Recherche du DNS académique/d'intérêt public
Contacts techniques sur la liste	Protection des données personnelles

Contacts administration sur la liste	Contrôle du nom de domaine Recherche du DNS académique/d'intérêt public Exécution des contrats/règlementation Achat/vente de nom de domaine
Contacts juridiques sur la liste	Contrôle du nom de domaine Recherche du DNS académique/d'intérêt public Actions juridiques Exécution des contrats/règlementation
Contacts commerciaux sur la liste	Recherche du DNS académique/d'intérêt public Utilisation individuelle d'Internet Contrôle du nom de domaine
Contacts en cas d'abus sur la liste	Recherche du DNS académique/d'intérêt public Enquête policière et réduction des abus Contrôle du nom de domaine Recherche du DNS académique/d'intérêt public
Fournisseur de services en ligne	Résolution des problèmes techniques
Fournisseurs de services Op/Sec	Enquête policière & réduction des abus de DNS
Étude de l'organisation de parrainage	Recherche du DNS d'intérêt public
Personne/entité faisant l'objet d'une enquête	Exécution des contrats/règlementation
Client de services d'anonymisation / d'intermédiation	Achat ou vente des noms de domaine commerciaux Contrôle des noms de domaine Résolution de problèmes techniques Exécution des contrats/règlementation Protection des données personnelles
Fournisseur de services d'anonymisation / d'intermédiation	Enquête policière et réduction des abus Achat ou vente des noms de domaine commerciaux Contrôle des noms de domaine Recherche du DNS d'intérêt public Résolution de problèmes techniques Actions en justice Protection des données personnelles Exécution des contrats/règlementation Résolution des problèmes techniques
Fournisseur RDS	Toutes fins
Titulaire (de nom de domaine)	Toutes fins
Contact juridique du titulaire du nom de domaine	Actions en justice Exécution des contrats/règlementation
Bureau d'enregistrement	Achat ou vente des noms de domaine commerciaux Contrôle des noms de domaine Recherche du DNS d'intérêt public Utilisation individuelle d'Internet Actions en justice Protection des données personnelles Exécution des contrats/règlementation Résolution des problèmes techniques Enquête policière et réduction des abus
Registre	Toutes fins
Rapporteur du problème	Résolution des problèmes techniques
Chercheur	Recherche du DNS académique/d'intérêt public
Revendeur	Contrôle du nom de domaine Enquête policière et réduction des abus

Résolveur du problème	Résolution des problèmes techniques
Cible de l'action civile/en justice	Utilisation individuelle d'Internet
Tierces parties cherchant un contact	Actions en justice
	Protection des données personnelles
Approbateur identifiant sécurisé	Protection des données personnelles
Destinataire identifiant sécurisé	Protection des données personnelles
Membres du panel UDRP	Exécution des contrats/règlementation
Fournisseur UDRP	Exécution des contrats/règlementation
Validateur	Toutes fins
Victime d'abus	Enquête policière & réduction des abus de DNS
Fournisseur d'hébergement sur le Web	Résolution des problèmes techniques

Tableau 4. Résumé représentatif des parties prenantes

e. Principes des contacts basés sur l'objectif

L'existence et l'utilisation de noms de domaine sur Internet dans des zones publiques créent des impacts externes potentiels sur des tierces parties au niveau mondial. Qu'il s'agisse de comportement abusif, de problèmes techniques, de violation de droits et de questions liées à des noms de domaine de plus ou moins grande importance, il existe une multitude de raisons pour qu'une tierce partie située quelque part dans le monde ait un besoin légitime de contacter une personne ou une organisation associée à un nom de domaine spécifique.

Par ailleurs, les titulaires de noms de domaine peuvent souhaiter et avoir le droit (selon leur juridiction locale) à la confidentialité. Il est possible qu'ils ne veuillent pas rendre leurs coordonnées de contact publiques. De plus, souvent, les titulaires de noms de domaine ne sont pas la personne ou l'entité appropriée pour résoudre un problème éventuellement soulevé par une tierce partie - par exemple, des problèmes liés à configuration DNS d'un nom de domaine ou une réponse à un litige à propos d'une marque de commerce. Ainsi, le fait de fournir les coordonnées du titulaire du nom de domaine uniquement ne satisfera probablement pas les tierces parties souhaitant résoudre des problèmes liés à un nom de domaine.

La nature variée des problèmes potentiels peut nécessiter des réponses différentes - du point de vue contenu et délais - à des situations souvent logiquement résolues par des personnes différentes et/ou des organisations associées à un nom de domaine spécifique. Toutefois, un nom de domaine doit au moins avoir les coordonnées d'un ou plusieurs contacts publiées de manière précise et joignable afin de répondre à des demandes externes et fournir un point de référence pour des objectifs admissibles d'acteurs externes touchés par l'existence ou les opérations d'un nom de domaine.

Le délai de réponse peut être un but souhaité pour la définition de politiques relatives à des types de contact spécifiques. Toutefois, ce but doit être équilibré par rapport aux charges que des exigences de réponse pourraient créer pour les entités remplissant ces

rôles. La manipulation du système, les requêtes inappropriées ou la surcharge délibérée des contacts ne devraient pas conduire à une pénalisation de ces contacts. Pour certains objectifs, il est souhaitable que les requérants disposent d'un processus à suivre en cas de problème de communication avec un contact qui ne répond pas (par ex. dans le cas d'abus, lorsqu'il faut répondre aux déclarations UDRP). L'absence de réponse à un tel processus pourrait potentiellement conduire à la suspension et/ou la suppression de ce contact et potentiellement affecter le nom de domaine dans un processus codifié. Cependant, les objectifs de politique spécifiques concernant les délais de réponse dépassent le champ du présent rapport.

Nº.	Principes des contacts basés sur l'objectif
8.	Au moins un contact basé sur l'objectif (PBC) doit être fourni pour chaque nom de domaine enregistré qui rend public l'ensemble de tous les éléments de données obligatoires pour tous les PBC obligatoires. Ce PBC doit être précis du point de vue syntaxe et joignable du point de vue fonctionnel afin de répondre aux besoins de tout objectif admissible codifié.
9.	Durant l'enregistrement d'un nom de domaine, l'identifiant[6] (ID) du contact du titulaire du nom de domaine doit être utilisé en tant qu'ID PBC par défaut pour chaque objectif. Le titulaire du nom de domaine doit être informé de tous les objectifs admissibles et avoir la possibilité de publier d'autres ID PBC pour chaque objectif, y compris de remplacer l'identifiant d'un contact du titulaire pour un objectif donné ou pour tous les objectifs.
10.	Il n'est pas nécessaire que le contact basé sur l'objectif soit le titulaire du nom de domaine et l'accès aux informations relatives au titulaire du nom de domaine peuvent rester hautement sécurisées comme pour d'autres politiques. Il faudrait noter que le PBC ne doit pas nécessairement représenter une personne mais peut être un point de contact désigné pour divers objectifs.
11.	Un nom de domaine ne doit pas être activé (introduit dans le DNS mondial) avant qu'une ID PBC ne soit fournie pour chaque objectif applicable. Si un PBC ne correspond plus à son objectif désigné, il faudrait avoir un processus qui permette au titulaire du nom de domaine de spécifier un nouveau contact

[6] Les ID des contacts sont des identifiants associés à des blocs de données de contact pour permettre l'édition et l'actualisation, présentés dans la section IV(a), éléments de données et définis dans la section V(d), cadre opérationnel pour les ID des contacts.

Nº.	Principes des contacts basés sur l'objectif
	valide, en donnant une notification et un délai raisonnables pour que cette ID PBC soit mise à jour. Selon le principe numéro 9 ci-dessus, l'identifiant (ID) du contact du titulaire du nom de domaine doit être utilisé en tant que ID PBC pour chaque objectif. L'absence de fourniture d'une ID PBC valide après ce délai pourrait mener à une suspension et/ou une suppression du nom de domaine dans un processus codifié. (voir section V pour les exigences de validation).
12.	L'ID PBC peut être éventuellement fourni pour chaque objectif admissible, avec des exigences définies qui varient concernant les éléments de données qui devraient être recueillis et publiés pour chaque type de PBC afin de satisfaire les besoins des objectifs admissibles associés.
13.	Un processus et des politiques doivent être élaborées pour permettre aux contacts désignés du titulaire du nom de domaine de consentir ou non (opt-in/opt-out) à avoir leurs ID de contact publiées en tant qu'ID PBC pour les noms de domaine, soutenir les droits les personnes et des entités d'accepter ou de rejeter la responsabilité d'accomplir des rôles spécifiques pour des enregistrements de noms de domaine spécifiques.
14.	Tout système fournissant des « contacts basés sur des objectifs » doit être flexible et permettre la création de nouveaux objectifs et types de contacts et leur publication dans le RDS. (voir section III(c) pour plus d'informations concernant l'ajout de nouveaux objectifs).

f. Rôles et responsabilités des contacts basés sur les objectifs

Tel que résumé dans la figure 4 et détaillé dans le tableau 1, l'EWG a analysé des cas d'utilisation représentatifs pour identifier les types d'utilisateurs qui souhaiteraient un accès à des données d'enregistrement de gTLD et les objectifs admissibles actuellement desservis par ces données. Pour accorder un accès basé sur l'objectif à des données d'enregistrement, tous les objectifs admissibles ont été attribués à des PBC. Par exemple :

- Un contact « juridique » peut être désigné pour traiter les litiges de marque commerciale ou d'autres plaintes juridiques concernant un nom de domaine. Pour permettre le contact à des fins associées, ce PBC doit simplement avoir une adresse physique pouvant recevoir des notifications juridiques, une adresse email pour recevoir des demandes et un numéro de téléphone ou de télécopie pour recevoir les questions.

- Un contact « en cas d'abus » peut être désigné pour traiter les demandes concernant des comportements abusifs provenant d'un nom de domaine et se manifestant dans le trafic ou d'autres activités Internet malveillantes hautement sensibles au facteur temps. Pour permettre le contact à des fins associées, ce PBC doit simplement avoir une adresse email pouvant recevoir et répondre à des plaintes valides et un numéro de téléphone actif pour recevoir les demandes. Le PBC peut aussi inclure des adresses de médias sociaux ou de messagerie instantanée pour faciliter l'interaction en temps réel, une adresse physique ou un numéro de télécopie pour recevoir les questions et une URL publiée qui facilite le signalement d'abus.

Les PBC sont aussi recommandés pour désigner les contacts administratif, technique, commercial et du fournisseur de services d'anonymisation/d'intermédiation accrédité. Une liste complète des types et des responsabilités des PBC est fournie dans le tableau 5 ; voir aussi section IV, principe de collecte de données no. 20, pour les besoins en éléments de données pour chaque type de PBC.

Tel qu'illustré dans la figure suivante, l'EWG recommande que la propre ID du titulaire du nom de domaine soit utilisée si des PBC plus spécifiques ne sont pas fournis pour un nom de domaine donné. Par exemple, si le contact juridique n'a pas été spécifié pour un nom de domaine donné, le titulaire du nom de domaine devrait être informé que des parties pourraient avoir besoin de les contacter à cette fin admissible et avoir la possibilité de désigner un PBC pour recevoir de telles requêtes concernant ce nom de domaine.

Si le titulaire choisit de ne pas désigner un PBC, de telles requêtes seront envoyées au titulaire du nom de domaine, en utilisant les données requises pour cet objectif associées à l'ID de contact du titulaire du nom de domaine. Si le titulaire du nom de domaine préfère ne pas rendre publics ces éléments de données, le nom de domaine peut être enregistré en utilisant un service d'anonymisation/d'intermédiation (PP). Voir section IV pour plus de détails sur les principes des éléments de données et les PBC.

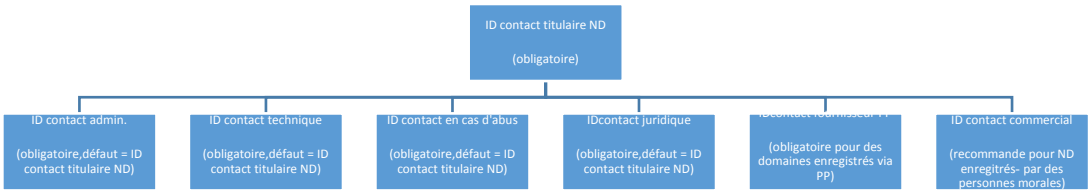


Figure 4. Types de contact RDS

Tous les objectifs/contacts doivent être codifiés par les décideurs de politiques via un processus défini pour ajouter, modifier ou supprimer des objectifs.

L'approche PBC privilégie la simplicité pour les titulaires de noms de domaine avec des besoins de contact basiques et offre un niveau de détail supplémentaire pour les titulaires de noms de domaine ayant des besoins de contact plus considérables. Afin d'illustrer ce concept, trois exemples différents fictifs mais typiques sont donnés ci-dessous :

1. Un titulaire de nom de domaine peut explicitement désigner son ID de contact titulaire en tant que seul point de contact pour son nom de domaine. Dans ce cas, les requêtes RDS pour chaque objectif admissible rendront des éléments de données autorisés publics ou sécurisés associés à l'ID de contact du titulaire, selon l'objectif.

Exemple de dossier de ND:

```
ID de contact du titulaire = <reg>
ID de contact technique = <reg>
ID de contact admin. = <reg>
ID de contact en cas d'abus = <reg>
ID de contact juridique = <reg>
```

2. Un titulaire de nom de domaine utilisant un service accrédité de **confidentialité** (défini dans la section VII) peut désigner plusieurs ID de contact unique pour son nom de domaine, y compris l'ID de contact du fournisseur de services d'anonymisation/d'intermédiation (c'-à-d. le fournisseur de services de confidentialité), un ID de contact technique (c'-à-d. le fournisseur d'hébergement ou FSI), et les ID des contact administratif, technique, en cas d'abus et juridique du fournisseur de services d'anonymisation/d'intermédiation. Dans cet exemple, le contact technique désigné est responsable de résoudre toutes les questions techniques associées au nom de domaine et le contact du fournisseur accrédité de services d'anonymisation/d'intermédiation est responsable de tous les services de confidentialité associés au nom de domaine (y compris la transmission de messages de contact admin., en cas d'abus et juridique au titulaire du nom de domaine).

Exemple de dossier de ND:

```
ID de contact du titulaire = <reg>
ID de contact PP = <pp>
ID de contact technique = <isp>
ID de contact admin. = <reg@pp>
ID de contact en cas d'abus = <reg@pp>
ID de contact juridique ID = <reg@pp>
```

3. Un titulaire de nom de domaine qui a choisi de s'identifier en tant que personne morale peut fournir plusieurs ID de contact unique pour un nom de domaine donné, y compris les ID PBC juridique, en cas d'abus et commercial spécifiquement associés à ce nom de domaine. Dans cet exemple, les requêtes RDS pour chacun de ces objectifs rendront des éléments de données associés à l'ID PBC correspondant spécialisé, facilitant un contact direct avec la personne ou l'entité qui a accepté d'assumer la responsabilité du rôle désigné. Ce scénario peut devenir plus usuel au fil du temps à mesure que les grandes organisations tireront parti de ce niveau de détail pour améliorer la 'joignabilité' et réduire la mauvaise communication et la redirection.

Exemple de dossier de ND:

```
ID de contact du titulaire = <reg>
ID de contact technique = <isp>
ID de contact admin. = <admin@reg>
ID de contact en cas d'abus = <abuse@reg>
ID de contact juridique = <legal@reg>
ID de contact commercial = <cs@reg>
```

Ces exemples sont illustrés par graphique dans la figure suivante :

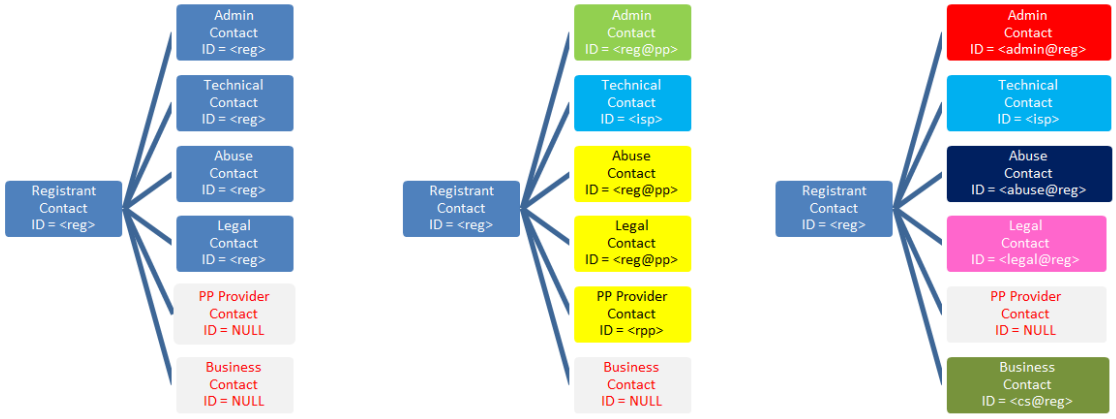


Figure 5. Exemple d'enregistrement de nom de domaine utilisant des contacts basés sur les objectifs

Se référer à la section IV pour une liste des PBC recommandés et à l'annexe D pour une liste complète des éléments de données associés à chaque objectif admissible et PBC y lié.

Les responsabilités du PBC comprennent recevoir les demandes relatives à ce nom de domaine, évaluer ces demandes et accuser réception de la demande et/ou notifier le titulaire/détenteur de licence, selon l'accord contractuel entre le titulaire du nom de domaine et le PBC.

Les responsabilités potentielles pour chaque PBC peuvent être résumées comme suit :

Type de PBC	Responsabilités potentielles
Admin.	Traiter les demandes liées à l'acquisition et à la vente de noms de domaine, telles que questions relatives à l'achat et au transfert du nom de domaine.
Juridique	Traiter les demandes concernant ce nom de domaine provenant des autorités fiscales, des enquêteurs UDRP, des enquêteurs sur la conformité contractuelle et des représentants légaux.
Technique	Traiter les demandes concernant ce nom de domaine liées à des pannes de sites Web, des problèmes de DNS, des problèmes de réception de courriel, etc.
Abus	Traiter les signalements d'abus du DNS concernant ce nom de domaine, y compris l'hameçonnage, les pourriels et autres activités

Type de PBC	Responsabilités potentielles
	nuisibles sur Internet.
Anonymisation intermédiation	Traiter les demandes de relais/divulgation, déposer des plaintes concernant l'abus de nom de domaine pour le compte du titulaire du nom de domaine/détenteur de licence, se conformer aux enquêtes des LEA concernant des activités criminelles.
Commercial	Traiter les demandes de consommateurs pour des informations relatives à une entreprise et des informations permettant de contacter l'entreprise pour de plus amples détails ou la résolution de plaintes de consommateurs.

Tableau 5. Responsabilités potentielles pour chaque contact basé sur un objectif

A envisager à l'avenir : Il pourrait y avoir de multiples PBC spécifiés pour chaque type de PBC, permettant un contact direct avec des personnes spécifiques ayant des responsabilités cruciales. Par exemple, pour une vaste présence sur Internet, il serait souhaitable de répartir les questions techniques parmi le postmaster, l'opérateur DNS, le webmaster, etc. Les devoirs exécutés par ces contacts spécialisés seraient libellés dans un champ qui serait publié dans les données publiques pour identifier l'objectif spécifique pour le PBC tel que désigné par le titulaire du ND. Cette complexité n'est probablement pas à l'ordre du jour mais devrait pouvoir être écartée à l'avenir.

g. Autorisation d'usage de contact RDS

Tel que décrit ci-dessus, les enregistrements de noms de domaine doivent désigner au moins les PBC requis. De tels contacts doivent être au courant et d'accord pour assumer le(s) rôle(s) désigné(s) pour chaque nom de domaine enregistré. Les principes associés à ce concept sont détaillés ci-dessous.

Nº.	Principes d'autorisation d'usage de contact basé sur l'objectif
15.	Chaque approbation de PBC doit pouvoir être obtenue de manière évolutive en temps réel ou quasi-réel pour éviter de retarder les enregistrements ou les mises à jour de noms de domaine.
16.	Les politiques et les processus doivent empêcher l'utilisation non autorisée de PBC.
17.	Le PBC ou le titulaire du nom de domaine doit pouvoir annuler une approbation plus tard. (Voir section V, validation pour détails)

Nº.	Principes d'autorisation d'usage de contact basé sur l'objectif
18.	Les titulaires de noms de domaine doivent pouvoir facilement se désigner eux-mêmes comme PBC pour leurs noms de domaine sans approbation externe/de tierce parties.

Par exemple, un titulaire de nom de domaine fournit un ID de contact PBC et un signal à usage unique qui peut être instantanément et automatiquement vérifié par le validateur responsable de cet ID de contact. Ou encore, un système de vérification par email ou message texto pourrait être employé dans un processus permettant d'obtenir l'autorisation de contact.

IV. Améliorer la responsabilité

Le RDS recommandé prend une approche nouvelle, en abandonnant le système actuel unique WHOIS en faveur d'un accès orienté sur les objectifs pour des données validées dans l'espoir d'améliorer la vie privée, l'exactitude et la responsabilité .

L'EWG estime qu'un paradigme d'accès sécurisé pourrait augmenter la responsabilité pour toutes les parties impliquées dans la divulgation et l'usage des données d'enregistrement des noms de domaine des gTLD. D'abord, le RDS enregistrerait tous les accès aux données d'enregistrement de gTLD, y compris les accès non authentifiés à des éléments de données publics et les restrictions d'accès afin de décourager les téléchargements de masse. De plus, l'accès sécurisé à des éléments de données plus sensibles 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. Enfin, le RDS vérifierait les accès aux données publiques et sécurisées pour minimiser les abus et imposerait des pénalités et autres sanctions en cas d'utilisation inappropriée. Différentes conditions peuvent être appliquées à différents objectifs. Si les requérants enfreignent les conditions établies, des pénalités seraient appliquées.

Plusieurs des membres de la communauté de l'ICANN ont exprimé leur inquiétude quant à abandonner un WHOIS public entièrement anonyme en faveur du paradigme d'accès sécurisé recommandé par l'EWG. Certains ont suggéré que toutes les données d'enregistrement devraient rester publiques pour des requérants entièrement anonymes, tandis que d'autres ont suggéré que peu ou pas de données devraient être publiques. Certains soutenaient le concept d'accréditation d'utilisateurs demandant un accès pour des objectifs admissibles mais souhaitaient plus de détails concernant les éléments de données disponibles, les processus d'accréditation et la façon d'établir des politiques concernant les objectifs admissibles et d'affiner ces politiques au fil du temps. Alors qu'il n'existe pas de réponse facile pour satisfaire ces points de vue différents, cette section présente en détail les recommandations de l'EWG dans ces domaines.

a. Principes des éléments de données

L'EWG recommande les principes suivants pour classifier les éléments de données.

Nº.	Principes des éléments de données
19.	Le RDS doit prévoir la divulgation d'éléments de données orientée sur un objectif. (Voir section III pour une liste des objectifs admissibles et des contacts basés sur des objectifs y associés (PBCs)).
20.	Toutes les informations collectées ne seront pas publiques ; leur divulgation doit dépendre du requérant et de l'objectif poursuivi.
21.	L'accès public à un ensemble minimum de données identifié doit être disponible, y compris les données des PBC publiées explicitement pour faciliter la communication pour cet objectif.
22.	Les éléments de données s'étant avérées sensibles (suite à l'évaluation de risque et d'impact) doivent être protégées au moyen d'un accès sécurisé, basé sur : • L'identification d'un objectif admissible • La divulgation du requérant/de son objectif • La mise en place d'audits / actions de conformité afin d'assurer que l'accès sécurisé ne fait pas l'objet d'abus.
23.	Seuls les éléments de données admissibles dans le cadre de l'objectif énoncé doivent être divulguées (c'-à-d. inclus dans des réponses ou recherchés à l'aide de requêtes inverses ou WhoWas).
24.	Les seuls éléments de données qui doivent être collectés sont ceux qui font l'objet d'au moins un objectif admissible.
25.	Chaque élément de données doit être associé à un ensemble d'objectifs admissibles. • Un ensemble initial d'utilisations acceptables, d'objectifs admissibles et de besoins d'éléments de données est identifié dans le présent rapport (voir section III et annexe D). • Chaque objectif admissible doit être associé à un accès à des éléments de données et des politiques d'utilisation clairement définis. • Tel que spécifié dans la section III, un processus de révision continu doit être défini pour prendre en considération de nouveaux objectifs proposés et mettre périodiquement à jour les objectifs admissibles afin de refléter les ajouts approuvés, en les attribuant à des éléments de données existants. • Un processus de définition de politique doit être défini pour prendre en considération les nouveaux éléments de données proposés et, si

Nº.	Principes des éléments de données
	nécessaire, actualiser les éléments de données définis, les attribuant à des objectifs admissibles existants.
26.	La liste des éléments de données minimum à collecter, stocker et divulguer doit être basée sur des cas d'utilisation connus (reflétés dans ce document) et une évaluation du risque (à compléter avant la mise en œuvre du RDS).
27.	Tous les registres et validateurs doivent stocker l'ensemble complet des éléments de données qu'ils recueillent/fournissent au RDS. (Voir aussi section VII, modèles de RDS possibles.)

Étape 1 : Collecte de données

Les données doivent être collectées avant de pouvoir être divulguées de manière sélective pour des objectifs admissibles. Les principes suivants sont recommandés pour guider la collecte au moment de l'enregistrement :

Nº.	Principes de collecte des données
28.	En appui aux principes juridiques globaux indiqués dans la section VI, les bureaux d'enregistrement et validateurs devraient offrir aux titulaires de noms de domaine et contacts basés sur les objectifs la possibilité, lors de la collecte de données, de consentir à l'utilisation de leurs données pour des objectifs admissibles pré-divulgués, conformément aux lois de protection des données de leur juridiction. A l'heure de formuler la politique, ce principe doit être abordé dans le cadre plus vaste du contexte de ces principes juridiques globaux.[7]
29.	Afin de satisfaire les besoins de contrôle du domaine de base, il faut qu'il soit obligatoire pour les registres et les bureaux d'enregistrement de recueillir et pour les titulaires de noms de domaine de fournir les éléments de données suivants lors de l'enregistrement d'un nom de domaine : a. Nom de domaine b. Serveurs DNS c. Nom du titulaire du nom de domaine d. Type de titulaire de nom de domaine Indique le type d'entité identifiée par le nom du titulaire du nom de domaine, pour utilisation lors de l'application des exigences relatives aux données d'enregistrement, comme suit :

[7] L'appui de ce texte était quasi unanime, un seul membre de l'EWG n'était pas d'accord.

Nº.	Principes de collecte des données
	Non déclarée – s'applique par défaut si aucune des options suivantes n'est sélectionnée et devra être traitée par le RDS de manière similaire à une personne physique. **Fournisseur d'anonymisation/d'intermédiation** – doit être sélectionnée pour des noms de domaine enregistrés en utilisant un fournisseur d'anonymisation/d'intermédiation accrédité. Lorsque cette option est sélectionnée, l'ID de contact d'un fournisseur d'anonymisation/d'intermédiation accrédité doit aussi être fourni pour permettre à une demande de relais/divulgation de parvenir au PBC PP. **Personne morale** – peut être sélectionnée pour des noms de domaine enregistrés par des entités qui ne sont PAS des personnes physiques NI des fournisseurs PP. Lorsque cette option est sélectionnée, l'ID de contact d'un PBC commercial désigné doit aussi être fourni pour faciliter les demandes et plaintes des consommateurs. (Voir note sous ce tableau). **Personne physique** – peut être sélectionnée pour des noms de domaine enregistrés par des personnes physiques Lorsque cette option est sélectionnée, ni le PBC PP ni le PBC commercial ne devront être définis et les nom et adresses du titulaire du nom de domaine devront être traités comme des informations personnelles conformément aux lois sur la protection des données applicables dans la juridiction du sujet concerné. e. ID de contact du titulaire du nom de domaine Un ID unique attribué à chaque contact de titulaire du nom de domaine [nom et adresse] durant la validation (se référer à la section V pour une définition plus détaillée de l'ID du contact et comment il est créé par le biais d'un validateur et utilisé pour l'enregistrement du nom de domaine) f. Adresse postale du titulaire du nom de domaine Comprend les éléments de données suivants : rue, ville, état/province, code postal, pays (le cas échéant) g. Adresse électronique du titulaire du nom de domaine h. Numéro de téléphone du titulaire du nom de domaine Comprend les éléments de données suivants : numéro et indicatif (le cas échéant)
30.	a. Pour améliorer la confidentialité et la joignabilité du titulaire du nom de domaine, les bureaux d'enregistrement doivent recueillir et les titulaires de noms de domaine doivent fournir des contacts basés sur l'objectif (PBC) pour chaque nom de domaine enregistré. b. Les titulaires de noms de domaine peuvent facultativement désigner les

Nº.	Principes de collecte des données
	PBC de leur fournisseur de services d'anonymisation/d'intermédiation ou les PBC de tiers autorisés pour ces objectifs admissibles spécifiques (voir section III). c. Pour satisfaire les besoins de communication associés à chaque objectif admissible, les PBC créés par le biais d'un validateur et par la suite associés à un nom de domaine doivent satisfaire les exigences obligatoires minimum d'éléments de données suivantes : Contact technique : Adresse e-mail Contact administratif : organisation, adresse email Contact juridique : organisation, adresse email, téléphone, adresse postale Contact en cas d'abus : adresse email, numéro de téléphone Contact commercial[8]: organisation, adresse email Contact du fournisseur d'anonymisation/d'intermédiation[9]: organisation, adresse email, URL_contact, URL_abus d. Si un titulaire de nom de domaine ne désigne pas un PBC pour chaque objectif admissible obligatoire, le propre ID de contact du titulaire du nom de domaine doit être utilisé par défaut pour ces PBC. (Il faudrait noter que le titulaire du nom de domaine peut éviter ceci en utilisant un service d'anonymisation/d'intermédiation accrédité ou en désignant des PBC). Lorsque l'ID de contact du titulaire du nom de domaine est utilisé en tant qu'ID de PBC, les exigences de collecte et de divulgation des données du titulaire du nom de domaine peuvent être augmentées pour satisfaire les besoins d'éléments de données obligatoires de PBC mentionnés ci-dessus.
31.	Pour éviter de recueillir plus de données que nécessaire, toutes les autres données fournies par le titulaire du nom de domaine non énumérées dans les principes 29 ou 30 ci-dessus et utilisées pour au moins un objectif admissible doivent être facultativement recueillies à la discrétion du titulaire du nom de domaine. Les validateurs, les registres et les bureaux d'enregistrement doivent faire en sorte que ces données soient recueillies et entreposées si le titulaire du nom de domaine le souhaite.
32.	Pour maximiser la stabilité de l'Internet, les éléments de données obligatoires suivants doivent être fournis par les registres et les bureaux d'enregistrement au RDS :

[8] Le contact est uniquement obligatoire si le type de titulaire de ND = personne morale

[9] Le contact est uniquement obligatoire si le type de titulaire de ND = fournisseur PP

Nº.	Principes de collecte des données
	a. Statut de l'enregistrement b. Statut du client (établi par le bureau d'enregistrement) c. Statut du serveur (établi par le registre) d. Bureau d'enregistrement e. Juridiction du bureau d'enregistrement f. Juridiction du registre g. Langue de l'accord d'enregistrement h. Date de création i. Date d'expiration du bureau d'enregistrement j. Date de mise à jour k. URL du bureau d'enregistrement l. Numéro IANA du bureau d'enregistrement m. Numéro de téléphone de contact avec le bureau d'enregistrement en cas d'abus n. Adresse électronique de contact avec le bureau d'enregistrement en cas d'abus o. URL du site de plaintes Internic
33.	Pour des éléments de données spécifiques aux TLD, le registre TLD doit établir et publier une politique de collecte de données (en ligne avec ces principes globaux) et être responsable de toute validation de ces éléments de données spécifiques aux TLD.
34.	Les validateurs, les registres et les bureaux d'enregistrement peuvent recueillir, entreposer ou divulguer des éléments de données supplémentaires pour utilisation interne jamais partagée avec le RDS.[10]

[10] Les exemples comprennent l'adresse IP utilisée par le client au moment de l'enregistrement, un lien vers la création d'une clé de transfert EPP pour un nom de domaine et les données de paiement associées au compte du client. Les données à utilisation interne ne sont pas normalisées par le RDS mais définies en privé par les registres et les bureaux d'enregistrement.

Note : Après beaucoup de discussions, l'EWG n'a pas recommandé d'ajouter un **objectif de nom de domaine** en tant qu'élément de données. Au lieu de cela, l'EWG a recommandé des principes pour réaliser les objectifs associés et un **PBC commercial** explicite qu'il est recommandé aux titulaires de noms de domaine de publier lorsqu'ils s'identifient comme **personnes morales** engagées dans des activités commerciales. Ceci pourrait résulter en la publication plus uniforme d'éléments de données de la part de nombreux utilisateurs commerciaux d'Internet afin d'encourager la confiance des consommateurs tout en reconnaissant que les titulaires de noms de domaine choisissent finalement eux-mêmes cette classification et qu'il serait pratiquement impossible de mettre en application au niveau mondial une conformité rigoureuse concernant un objectif de nom de domaine = commercial vs. non commercial.

Étape 2 : Divulgation de données

Une fois les données collectées, elles peuvent être divulguées de manière sélective pour des objectifs admissibles. Les principes suivants sont recommandés pour guider la divulgation lorsque les requêtes sont reçues :

Nº.	Principes de divulgation de données
35.	Pour privilégier au maximum la vie privée des titulaires de noms de domaine, les données fournies par le titulaire du nom de domaine doivent être sécurisées par défaut, sauf lorsqu'il y a un besoin irréfutable pour un accès public qui va au-delà des risques résultants. • Les titulaires des noms de domaine peuvent choisir de rendre publiques toutes données sécurisées fournies par le titulaire du nom de domaine suite à un consentement préalable.
36.	Pour maximiser la stabilité de l'Internet, toutes les données d'enregistrement fournies par les registres ou les bureaux d'enregistrement doivent être toujours publiques, sauf si ce fait résulte en un risque inacceptable. • Les titulaires des noms de domaine peuvent choisir de sécuriser toutes données publiques fournies par les registres/bureaux d'enregistrement, sauf comme il est noté ci-dessous pour permettre un contrôle de nom de domaine de base.
37.	Pour maximiser la joignabilité, tous les PBC doivent être public par défaut.

Nº.	Principes de divulgation de données
	• Les détenteurs de contact[11] peuvent choisir de sécuriser tout élément de données PBC, sauf ceux requis pour satisfaire l'objectif désigné (plus de détails au Tableau 5).
38.	Pour satisfaire les besoins de contrôle de noms de domaine de base, les données suivantes fournies par le titulaire du nom de domaine, qu'il est obligatoire de collecter et dont la divulgation est à bas risque, doivent être inclues dans l'ensemble de données publiques minimum : a. Nom de domaine b. Serveurs DNS c. Type de titulaire de nom de domaine d. ID contact titulaire de nom de domaine (définie à la section V) e. Adresse email du titulaire du nom de domaine f. ID du contact technique g. ID du contact admin. h. ID du contact juridique i. ID du contact en cas d'abus j. ID contact fournisseur PP (obligatoire uniquement si le type de titulaire de ND = fournisseur PP) k. ID contact commercial (obligatoire uniquement obligatoire si le type de titulaire de ND = personne morale)
39.	Pour un équilibre entre la simplicité et la joignabilité, si le titulaire du nom de domaine ne fournit pas de PBC obligatoire, il doit être informé que son ID de contact sera utilisé en tant que PBC, et les éléments de données du titulaire du nom de domaine seront publiés en tant que contacts technique, admin., juridique et en cas d'abus relatifs à ce nom de domaine. Le titulaire du nom de domaine peut éviter cette dovulgation en spécifiant un ou plusieurs PBC tiers ou en utilisant un service d'anonymisation/d'intermédiation accrédité (dans ce cas, ces adresses seront fournies par le fournisseur de services).

[11] Selon la section III(g), autorisation d'utilisation de contact RDS, les PBC désignés doivent autoriser l'utilisation d'une ID de contact dans le cadre de l'enregistrement d'un nom de domaine donné. En ce faisant, les détenteurs de contact conviennent aussi de l'utilisation publique/sécurisée de leurs données dans cet objectif. Toutefois, si un PBC pré-validé ne contient pas les éléments de données publics/obligatoires pour satisfaire un objectif donné, ce PBC ne peut pas être désigné pour cet objectif dans l'enregistrement d'un nom de domaine.

Nº.	Principes de divulgation de données
40.	Pour des éléments de données spécifiques aux TLD, le registre TLD doit établir et publier une politique de divulgation de données (en ligne avec ces principes globaux) et être responsable de l'identification des objectifs admissibles pour tous éléments de données sécurisés spécifiques aux TLD.

Classifications des éléments de données résultant de ce qui précède

Sur la base de ces principes, le tableau suivant présente en détail la classification résultant pour chaque élément de données RDS recommandé par l'EWG, utilisant le système de notation suivant :

- si la collecte de l'élément est obligatoire (M) ou facultative (O). Ceci signifie :

  [1] Pour les données recueillies des titulaires de ND,
  (M)obligatoires signifie que les données doivent être requises par les bureaux d'enregistrement/validateurs et fournies par les titulaires de ND, tandis que (O)facultatives signifie que les données doivent être requises par le bureau d'enregistrement/validateur mais peuvent être ou ne pas être fournies à la discrétion du titulaire du nom de domaine, selon le cas.

  [2] Pour les données recueillies des détenteurs de PBC,
  (M)obligatoires signifie que les données doivent être requises par les bureaux d'enregistrement/validateurs et fournies par les détenteurs de contact, tandis que (O)facultatives signifie que les données doivent être requises par le bureau d'enregistrement/validateur mais peuvent être ou ne pas être fournies à la discrétion du détenteur de contact, selon le cas, et

  (R)ecommandé signifie que les données doivent être requises par le bureau d'enregistrement/validateur mais peuvent être ou ne pas être fournies à la discrétion du détenteur de contact, selon le cas, pour refléter les recommandations de « meilleures » et de « bonnes » pratiques[12]

[12] Les meilleures pratiques recommandées pour la publication des divers éléments de données de PBC se basent sur l'expérience opérationnelle des membres de l'EWG. Les éléments obligatoires représentent l'exigence opérationnelle minimum pour réaliser ces objectifs. Toutefois, en pratique, s'il existe une méthode de communication pour un objectif donné (par ex. un formulaire en ligne pour signaler des problèmes, une autre adresse email pour joindre le personnel technique), alors une méthode alternative est hautement utile et souvent préférée dans le traitement des problèmes . Ceci va varier selon les PBC - par exemple, une adresse postale est plus utile pour des objectifs de contact juridique ou commercial et grandement inutile pour résoudre rapidement des objectifs de contact technique ou en cas d'abus. Ainsi, l'EWG a fait des recommandations spécifiques pour des éléments de données dans chaque type de PBC.

[3] Pour les données fournies par les registres et bureaux d'enregistrement au RDS,
(M)obligatoires signifie que les données doivent être fournies par le registre/bureau d'enregistrement, tandis que
(O)facultatives signifie que les données peuvent être ou ne pas être fournies, selon le cas.

- Si chaque élément est (P)ublic [accessible à chacun, avec ou sans authentification] ou (G)sécurisé [accessible uniquement aux utilisateurs authentifiés, uniquement pour des objectifs admissibles] et si les titulaires de ND peuvent modifier ce paramètre de divulgation par défaut (Y/N). Ceci signifie :

  [4] Pour les données recueillies des titulaires de ND,
  P / N signifie que les données recueillies doivent être publiques et ne peuvent pas être masquées,
  P / Y signifie que les données recueillies sont publiques par défaut mais peuvent être masquées par le titulaire du nom de domaine,
  G / Y signifie que les données recueillies sont sécurisées par défaut mais peuvent être rendues public par le titulaire du ND, suite à un consentement préalable.

  [5] Pour les données fournies par les registres et les bureaux d'enregistrement au RDS,
  P / N signifie que les données fournies doivent être publiques et ne peuvent être masquées tandis que
  G / N signifierait que les données fournies doivent être sécurisées ; il n'y a pas d'éléments de données dans cette catégorie.

  [6] Pour les données recueillies des détenteurs de contacts basés sur l'objectif,
  P / N signifie que les données recueillies doivent être publiques et ne peuvent être masquées,
  P / Y signifie que les données recueillies sont publiques par défaut mais peuvent être masquées par le détenteur du contact

Il faudrait noter que le fait que des éléments de données sécurisés soient accessibles à un utilisateur donné dépend des objectifs admissibles. Lorsqu'un titulaire de nom de domaine choisit de rendre public un élément sécurisé par défaut, cet élément devient accessible à tous. Lorsqu'un titulaire de nom de domaine choisit de sécuriser un élément public par défaut, l'accès à cet élément est alors limité aux objectifs admissibles.

DONNÉES FOURNIES PAR LES REGISTRES/BUREAUX D'ENREGISTREMENT	Collecte M ou O	Divulgation Défaut P ou G	La divulgation peut être modifiée ?	Notes Voir [3] Définition de collecte et [5] Définition de divulgation
Statut de l'enregistrement	**M**	**P**	**N**	
Délégation DNSSEC	O	**P**	**N**	
Statut du client (bureau d'enregistrement)	**M**	**P**	**N**	Contient toutes les valeurs applicables au nom de domaine au niveau du bureau d'enregistrement SupressionInterdite, RenouvellementInterdit, TransfertInterdit
Statut du serveur (registre)	**M**	**P**	**N**	Pas dans le RAA, similaire à ci-dessus, mais au niveau du registre
Bureau d'enregistrement	**M**	**P**	**N**	
Revendeur	O	**P**	**N**	
Juridiction du bureau d'enregistrement	**M**	**P**	**N**	Pas dans le RAA
Juridiction du registre	**M**	**P**	**N**	Pas dans le RAA
Langue de l'accord d'enregistrement	**M**	**P**	**N**	Pas dans le RAA
Date de création	**M**	**P**	**N**	
Date de l'enregistrement initial	O	**P**	**N**	Pas dans le RAA
Date d'expiration du bureau d'enregistrement	**M**	**P**	**N**	
Date de mise à jour	**M**	**P**	**N**	
URL du bureau d'enregistrement	**M**	**P**	**N**	
Numéro IANA du bureau d'enregistrement	**M**	**P**	**N**	
Adresse électronique de contact avec le bureau d'enregistrement en cas d'abus	**M**	**P**	**N**	
Numéro de téléphone de contact avec le bureau d'enregistrement en cas d'abus	**M**	**P**	**N**	

DONNÉES FOURNIES PAR LES REGISTRES/BUREAUX D'ENREGISTREMENT	Collecte M ou O	Divulgation Défaut P ou G	La divulgation peut être modifiée ?	Notes Voir [3] Définition de collecte et [5] Définition de divulgation
URL du site de plaintes Internic	**M**	**P**	**N**	

DONNÉES DU TITULAIRE DE ND collectées auprès du titulaire du nom de domaine	Collecte M ou O	Divulgation Défaut P ou G	La divulgation peut être modifiée ?	Notes Voir [1] Définition de collecte et [4] Définition de divulgation
Nom de domaine	**M**	**P**	**N**	
Serveurs DNS	**M**	**P**	**N**	
Nom du titulaire du nom de domaine	**M**	G	Y	
Type de titulaire de nom de domaine	**M**	**P**	**N**	
ID de contact du titulaire du nom de domaine	**M**	**P**	**N**	Remplace l'ID du titulaire du ND dans le registre, émis par le validateur dans le RDS
Statut de validation du contact du titulaire du nom de domaine	**M**	**P**	**N**	Nouveau, fourni par le validateur
Horodatage dernière validation du contact du titulaire du nom de domaine	**M**	**P**	**N**	Nouveau, fourni par le validateur
Organisation du titulaire du nom de domaine	O	**P**	Y	Collecté quand le type de titulaire de ND = personne morale ou fournisseur d'intermédiation
Identifiant de l'entreprise du titulaire du ND (par ex. Nom commercial, D-U-N-S)	O	**P**	Y	Identifiants réels délivrés aux entreprises par des sources telles que Dunn et Bradstreet Collectés lorsque le type de titulaire de ND = personne morale Pas dans le RAA
Adresse de résidence du titulaire du nom de domaine	**M**	G	Y	
Ville du titulaire du nom de domaine	**M**	G	Y	
État / province du titulaire du nom de domaine	O	G	Y	Selon le RAA de 2013, tous les éléments « état/province » collectés le cas échéant
Code postal du titulaire du nom de domaine	O	G	Y	Selon le RAA de 2013, tous les éléments « code postal » collectés le cas échéant
Pays du titulaire du nom de domaine	**M**	G	Y	
Numéro de poste téléphonique du titulaire du nom de domaine	**M**	G	Y	Extension téléphonique le cas échéant

Numéro de poste téléphonique alternatif du titulaire du nom de domaine	O	G	Y	Nouvelle option, pas dans le RAA
Adresse électronique du titulaire du nom de domaine	**M**	**P**	**N**	
Adresse électronique alternative du titulaire du nom de domaine	O	**P**	Y	Nouvelle option, pas dans le RAA
Numéro de poste de télécopie du titulaire du nom de domaine	O	G	Y	Selon le RAA de 2013, tous les éléments « télécopie » et « poste de télécopie » collectés le cas échéant
Message texte du titulaire de nom de domaine	O	G	Y	Nouvelle option, pas dans le RAA
Messagerie instantanée du titulaire de nom de domaine	O	G	Y	Nouvelle option, pas dans le RAA
Médias sociaux du titulaire de nom de domaine	O	G	Y	Nouvelle option, pas dans le RAA
Médias sociaux alternatifs du titulaire de nom de domaine	O	G	Y	Nouvelle option, pas dans le RAA
URL de contact du titulaire de nom de domaine	O	G	Y	Nouvelle option, pas dans le RAA
URL en cas d'abus du titulaire de nom de domaine	O	G	Y	Nouvelle option, pas dans le RAA

CONTACTS BASÉS SUR LES OBJECTIFS Contact administratif	**Collecte M/R/O**	**Divulgation Défaut P ou G**	**La divulgation peut être modifiée ?**	**Notes** Voir [2] Définition de collecte et [6] Définition de divulgation
Buts : Achat/vente de ND, contrôle de nom de domaine, recherche du DNS				
ID du contact administratif	**M**	**P**	**N**	
ID du PBC	**M**	**P**	**N**	Pas dans le RAA
Statut de validation du PBC	**M**	**P**	**N**	Nouveau, fourni par le validateur
Horodatage dernière validation du PBC	**M**	**P**	**N**	Nouveau, fourni par le validateur
Nom du PBC	**M**	**P**	**N**	
Organisation du PBC	**M**	**P**	**N**	

Adresse de résidence du PBC	R	**P**	Y	
Ville du PBC	R	**P**	Y	
État / province du PBC	O	**P**	Y	
Code postal du PBC	O	**P**	Y	
Pays du PBC	**M**	**P**	**N**	
Numéro de poste téléphonique du PBC	O	**P**	Y	
Numéro de poste téléphonique alternatif du PBC	O	**P**	Y	Pas dans le RAA
Adresse électronique du PBC	**M**	**P**	**N**	
Adresse électronique alternative du PBC	O	**P**	Y	Pas dans le RAA
Numéro de poste télécopie du PBC	O	**P**	Y	
Messagerie texte du PBC	O	**P**	Y	Pas dans le RAA
Messagerie instantanée du PBC	O	**P**	Y	Pas dans le RAA
Médias sociaux du PBC	O	**P**	Y	Pas dans le RAA
Médias sociaux alternatifs du PBC	O	**P**	Y	Pas dans le RAA
URL de contact du PBC	O	**P**	Y	Pas dans le RAA
URL en cas d'abus du PBC	O	**P**	Y	Pas dans le RAA

CONTACTS BASÉS SUR LES BUTS Contact juridique	Collecte M/R/O	Divulgation Défaut P ou G	La divulgation peut être modifiée ?	Notes Voir [2] Définition de collecte et [6] Définition de divulgation
Buts : Actions en justice, règlementation/contrats, contrôle du nom de domaine, recherche du DNS				
ID du contact juridique	**M**	**P**	**N**	Pas dans le RAA
ID du PBC	**M**	**P**	**N**	Pas dans le RAA
Statut de validation du PBC	**M**	**P**	**N**	Nouveau, fourni par le validateur
Horodatage dernière validation du PBC	**M**	**P**	**N**	Nouveau, fourni par le validateur
Nom du PBC	**M**	**P**	**N**	
Organisation du PBC	**M**	**P**	**N**	
Adresse de résidence du PBC	**M**	**P**	**N**	
Ville du PBC	**M**	**P**	**N**	
État / province du PBC	O	**P**	Y	
Code postal du PBC	O	**P**	Y	
Pays du PBC	**M**	**P**	**N**	
Numéro de poste téléphonique du PBC	**M**	**P**	**N**	
Numéro de poste téléphonique alternatif du PBC	O	**P**	Y	Pas dans le RAA
Adresse électronique du PBC	**M**	**P**	**N**	
Adresse électronique alternative du PBC	O	**P**	Y	Pas dans le RAA
Numéro de poste télécopie du PBC	**R**	**P**	**Y**	
Messagerie texte du PBC	O	**P**	Y	Pas dans le RAA
Messagerie instantanée du PBC	O	**P**	Y	Pas dans le RAA
Médias sociaux du PBC	O	**P**	Y	Pas dans le RAA
Médias sociaux alternatifs du PBC	O	**P**	Y	Pas dans le RAA
URL de contact du PBC	O	**P**	Y	Pas dans le RAA
URL en cas d'abus du PBC	O	**P**	Y	Pas dans le RAA

CONTACTS BASÉS SUR LES BUTS Contact technique	Collecte M/R/O	Divulgation Défaut P ou G	La divulgation peut être modifiée ?	Notes Voir [2] Définition de collecte et [6] Définition de divulgation
Buts : Résolution de problèmes techniques, contrôle du nom de domaine, recherche du DNS				
ID du contact technique	**M**	**P**	**N**	
ID du PBC	**M**	**P**	**N**	Pas dans le RAA
Statut de validation du PBC	**M**	**P**	**N**	Nouveau, fourni par le validateur
Horodatage dernière validation du PBC	**M**	**P**	**N**	Nouveau, fourni par le validateur
Nom du PBC	R	**P**	Y	
Organisation du PBC	R	**P**	Y	
Adresse de résidence du PBC	R	**P**	Y	
Ville du PBC	R	**P**	Y	
État / province du PBC	O	**P**	Y	
Code postal du PBC	O	**P**	Y	
Pays du PBC	**M**	**P**	**N**	
Numéro de poste téléphonique du PBC	**R**	**P**	Y	
Numéro de poste téléphonique alternatif du PBC	**R**	**P**	Y	Pas dans le RAA
Adresse électronique du PBC	**M**	**P**	**N**	
Adresse électronique alternative du PBC	**R**	**P**	Y	Pas dans le RAA
Numéro de poste télécopie du PBC	O	**P**	Y	
Messagerie texte du PBC	**R**	**P**	Y	Pas dans le RAA
Messagerie instantanée du PBC	**R**	**P**	Y	Pas dans le RAA
Médias sociaux du PBC	O	**P**	Y	Pas dans le RAA
Médias sociaux alternatifs du PBC	O	**P**	Y	Pas dans le RAA
URL de contact du PBC	**R**	**P**	Y	Pas dans le RAA
URL en cas d'abus du PBC	O	**P**	Y	Pas dans le RAA

CONTACTS BASÉS SUR LES OBJECTIFS Contact en cas d'abus :	Collecte M/R/O	Divulgation Défaut P ou G	La divulgation peut être modifiée ?	Notes Voir [2] Définition de collecte et [6] Définition de divulgation
But : Réduction des abus, contrôle de nom de domaine, recherche du DNS				
ID du contact en cas d'abus	**M**	**P**	**N**	Pas dans le RAA
ID du PBC	**M**	**P**	**N**	Pas dans le RAA
Statut de validation du PBC	**M**	**P**	**N**	Nouveau, fourni par le validateur
Horodatage dernière validation du PBC	**M**	**P**	**N**	Nouveau, fourni par le validateur
Nom du PBC	R	**P**	Y	
Organisation du PBC	R	**P**	Y	
Adresse de résidence du PBC	R	**P**	Y	
Ville du PBC	R	**P**	Y	
État / province du PBC	O	**P**	Y	
Code postal du PBC	O	**P**	Y	
Pays du PBC	**M**	**P**	**N**	
Numéro de poste téléphonique du PBC	**M**	**P**	**N**	
Numéro de poste téléphonique alternatif du PBC	O	**P**	Y	Pas dans le RAA
Adresse électronique du PBC	**M**	**P**	**N**	
Adresse électronique alternative du PBC	O	**P**	Y	Pas dans le RAA
Numéro de poste télécopie du PBC	O	**P**	Y	
Messagerie texte du PBC	O	**P**	Y	Pas dans le RAA
Messagerie instantanée du PBC	**R**	**P**	Y	Pas dans le RAA
Médias sociaux du PBC	**R**	**P**	Y	Pas dans le RAA
Médias sociaux alternatifs du PBC	O	**P**	Y	Pas dans le RAA
URL de contact du PBC	**R**	**P**	Y	Pas dans le RAA
URL en cas d'abus du PBC	**R**	**P**	**Y**	Pas dans le RAA

CONTACTS BASÉS SUR LES BUTS Contact du fournisseur d'anonymisation/intermédiation (PP)	Collecte M/R/O	Divulgation Défaut P ou G	La divulgation peut être modifiée ?	Notes Voir [2] Définition de collecte et [6] Définition de divulgation
Buts : Protection des données personnelles, contrôle du nom de domaine, recherche du DNS				
ID du contact PP	**M**	**P**	**N**	Pas dans le RAA
ID du PBC	**M**	**P**	**N**	Pas dans le RAA
Statut de validation du PBC	**M**	**P**	**N**	Nouveau, fourni par le validateur
Horodatage dernière validation du PBC	**M**	**P**	**N**	Nouveau, fourni par le validateur
Nom du PBC	**M**	**P**	**N**	
Organisation du PBC	**M**	**P**	**N**	
Adresse de résidence du PBC	**M**	**P**	**N**	
Ville du PBC	**M**	**P**	**N**	
État / province du PBC	O	**P**	Y	
Code postal du PBC	O	**P**	Y	
Pays du PBC	**M**	**P**	**N**	
Numéro de poste téléphonique du PBC	**M**	**P**	**N**	
Numéro de poste téléphonique alternatif du PBC	O	**P**	Y	Pas dans le RAA
Adresse électronique du PBC	**M**	**P**	**N**	
Adresse électronique alternative du PBC	O	**P**	Y	Pas dans le RAA
Numéro de poste télécopie du PBC	O	**P**	Y	
Messagerie texte du PBC	O	**P**	Y	Pas dans le RAA
Messagerie instantanée du PBC	O	**P**	Y	Pas dans le RAA
Médias sociaux du PBC	O	**P**	Y	Pas dans le RAA
Médias sociaux alternatifs du PBC	O	**P**	Y	Pas dans le RAA
URL de contact du PBC	**M**	**P**	**N**	Pas dans le RAA
URL en cas d'abus du PBC	**M**	**P**	**N**	Pas dans le RAA

CONTACTS BASÉS SUR LES BUTS Contact commercial	Collecte M/R/O	Divulgation Défaut P ou G	La divulgation peut être modifiée ?	Notes Voir [2] Définition de collecte et [6] Définition de divulgation
Buts : Utilisation individuelle d'Internet, contrôle du nom de domaine, recherche du DNS				
ID du contact commercial	**M**	**P**	**N**	Pas dans le RAA
ID du PBC	**M**	**P**	**N**	Pas dans le RAA
Statut de validation du PBC	**M**	**P**	**N**	Nouveau, fourni par le validateur
Horodatage dernière validation du PBC	**M**	**P**	**N**	Nouveau, fourni par le validateur
Nom du PBC	**M**	**P**	**N**	
Organisation du PBC	**M**	**P**	**N**	
Adresse de résidence du PBC	**M**	**P**	**N**	
Ville du PBC	**M**	**P**	**N**	
État / province du PBC	O	**P**	Y	
Code postal du PBC	O	**P**	Y	
Pays du PBC	**M**	**P**	**N**	
Numéro de poste téléphonique du PBC	R	**P**	Y	
Numéro de poste téléphonique alternatif du PBC	O	**P**	Y	Pas dans le RAA
Adresse électronique du PBC	R	**P**	Y	
Adresse électronique alternative du PBC	O	**P**	Y	Pas dans le RAA
Numéro de poste télécopie du PBC	O	**P**	Y	
Messagerie texte du PBC	O	**P**	Y	Pas dans le RAA
Messagerie instantanée du PBC	O	**P**	Y	Pas dans le RAA
Médias sociaux du PBC	O	**P**	Y	Pas dans le RAA
Médias sociaux alternatifs du PBC	O	**P**	Y	Pas dans le RAA
URL de contact du PBC	**R**	**P**	**Y**	Pas dans le RAA
URL en cas d'abus du PBC	O	**P**	Y	Pas dans le RAA

L'EWG réitère aussi sa recommandation de réaliser une analyse des risques/impacts de champ élargi pour confirmer que ces classifications basées sur les principes résultent en fait en une collecte et une divulgation appropriées des données à des fins définies.

Alignement sur le RAA 2013 et nouveaux éléments de données

Pour faciliter la transition et la compréhension, les noms des éléments de données recommandés par l'EWG ont été alignés sur ceux identifiés dans le RAA 2013 dans la mesure du possible (par ex. délégation DNSSEC, date d'expiration du RDS). Toutefois, les noms des éléments de données utilisés dans le RAA 2013 pour les éléments de données de contact ne sont pas suffisants pour refléter la proposition de contacts basés sur les objectifs de l'EWG (voir section III). Pour parer à ce manque, l'EWG a appliqué les concordances suivantes :

> Lorsque l'ID de contact admin RDS se réfère à un PBC,
> Nom PBC RDS = Nom de contact admin RAA
> Organisation PBC RDS = Organisation contact admin RAA
> et ainsi de suite pour les autres éléments de données de contact admin du RAA
>
> Lorsque l'ID de contact technique RDS se réfère à un PBC,
> Nom PBC RDS = Nom du contact technique RAA
> Organisation PBC RDS = Organisation du contact technique RAA
> et ainsi de suite pour les autres éléments de données de contact technique du RAA

Note : L'EWG recommande que le portail RDS mette les définitions de chaque type de PBC directement à disposition des utilisateurs du RDS (par exemple, en utilisant des définitions qui apparaissent lorsque le curseur se trouve au-dessus du terme) pour indiquer clairement que les PBC sont publiés afin de traiter les demandes dans des objectifs admissibles et qu'un point de contact doit être désigné pour couvrir ces objectifs. Les titulaires de noms de domaine peuvent choisir de recevoir les demandes eux-mêmes (désigner l'ID du titulaire comme PBC), engager un fournisseur de services d'anonymisation/d'intermédiation pour recevoir ces demandes (engager un PP pour fournir ces éléments de données - d'habitude en transmettant les adresses ou les adresses du fournisseur) ou désigner une entité spécifique qui recevra ces demandes (par ex. un fournisseur de services, un fournisseur d'hébergement, un représentant juridique, un service clientèle).

Tous les éléments de données sont tel que défini dans le RAA 2013, avec les ajouts suivants :

Juridiction du bureau d'enregistrement et du registre : La juridiction légale dans laquelle opère le bureau d'enregistrement ou le registre, tel qu'indiqué dans l'accord qu'ils ont signé avec l'ICANN.

Langue de l'accord d'enregistrement : La langue dans laquelle est écrit le contrat entre le bureau d'enregistrement et le titulaire du nom de domaine.

Date de l'enregistrement initial : La date à laquelle ce nom de domaine a été initialement enregistré.[13]

Statut du client, statut du serveur : Développant les valeurs de statut du client du RAA 2013, ces éléments de données contiennent les valeurs de statut du bureau d'enregistrement (client) et du registre (serveur) actuellement appliquées à ce nom de domaine : SupressionInterdite, RenouvellementInterdit, TransfertInterdit.

Identifiant de l'entreprise du titulaire du nom de domaine : Le numéro de commerce RU, le numéro D-U-N-S ou un autre identifiant d'entreprise unique réel attribué au titulaire du nom de domaine par un annuaire commercial public. Ceci permet de rechercher une entreprise en dehors du RDS.

ID de contact du titulaire du nom de domaine : Un identifiant unique attribué à un bloc de données de contact pré-validé identifié comme titulaire de ce nom de domaine. Se référer à la section V pour une définition plus détaillée de l'ID de contact, comment il est créé et utilisé. Cet ID permet la réutilisation et l'entretien des données de contact au sein du RDS. Il faudrait noter que lorsque le type de titulaire de nom de domaine = Anonymisation/intermédiation, l'ID de contact du titulaire du nom de domaine reflètera l'identifiant unique attribué à ce fournisseur accrédité d'anonymisation/d'intermédiation.

Statut de validation de contact de PBC/titulaire de nom de domaine, Horodatage de dernière validation de contact PBC/titulaire de nom de domaine : Le plus haut niveau de validation obtenu et la date à laquelle de la validation la plus récente, tel que défini dans la section V.

Messagerie texte, messagerie instantanée, médias sociaux PBC/titulaire de nom de domaine : Les nouvelles méthodes de contact qui pourraient être facultativement utilisées pour joindre le titulaire du nom de domaine ou le PBC par texto, messagerie instantanée ou un vecteur de communication de médias sociaux.

Adresse électronique alternative, téléphone alternatif, médias sociaux alternatifs PBC/titulaire de nom de domaine : Nouvelles adresses alternatives qui pourraient être

[13] Ceci est différent de la date de création puisque la date de création reprend la dernière fois que le nom de domaine a été enregistré ; il est possible que le nom de domaine ait été auparavant enregistré et par la suite suite supprimé plusieurs fois. La date de l'enregistrement initial correspond à la première date à laquelle le nom de domaine a été enregistré.

facultativement utilisées pour joindre le titulaire du nom de domaine ou le PBC si l'adresse primaire ne fonctionne pas. Ces nouveaux éléments de données sont destinés à aborder les besoins communs tels que la résolution de problèmes techniques lorsque le nom de domaine lui-même n'est pas opérationnel et permettent un contact plus rapide via téléphone portable ou médias sociaux.

URL de contact, URL en cas d'abus du PBC/titulaire du nom de domaine Nouveaux éléments de données qui peuvent facultativement conduire à des pages Web où les instructions de contact ou de signalement d'abus, les politiques ou les formulaires peuvent être placés pour faciliter une communication plus productive.

ID de contact du PBC : Un identifiant unique attribué à un bloc de données de contact pré-validé identifié comme PBC pour ce nom de domaine, dans le rôle indiqué par le rôle du contact. L'ID de contact du titulaire du nom de domaine et l'ID de contact du PBC peuvent se référer au même contact.

Note : Les défis en matière de transition et de conformité associés à ces nouveaux éléments de données doivent être pris en considération avant toute mise en œuvre du RDS.

b. Principes pour l'accès aux données non authentifié et sécurisé

L'EWG recommande qu'une nouvelle approche soit adoptée pour l'accès aux données d'enregistrement, abandonnant complètement l'accès anonyme de tout le monde à tout en faveur d'un nouveau paradigme qui combine l'accès public à quelques données avec un accès sécurisé à d'autres données. Les principes qui reflètent cette recommandation suivent ci-après.

Nº.	Principes d'accès aux données
41.	Un ensemble minimum d'éléments de données, au moins aligné sur le régime de confidentialité le plus strict, doit être accessible aux utilisateurs non authentifiés du RDS.
42.	De multiples niveaux d'accès authentifié doivent être prévus, cohérents avec les objectifs admissibles stipulés.
43.	Les identifiants d'accès des utilisateurs du RDS doivent être liés à un processus d'accréditation contrôlable, tel que défini dans la section IV(c), accréditation d'utilisateur du RDS.
44.	L'accès ne doit pas être discriminatoire (c'est à dire, le processus doit établir des règles de jeu équitables pour tous les requérants ayant le même objectif).

Nº.	Principes d'accès aux données
45.	Pour décourager des usages inappropriés et pour promouvoir la responsabilité : • Tout accès à des éléments de données doit être basé sur un objectif énoncé ; • L'accès à des éléments de données sécurisés doit être limité à des requérants authentifiés qui affirment un objectif admissible et • Les requérants doivent pouvoir demander et recevoir des identifiants qu'ils pourraient utiliser dans d'autres demandes d'accès authentifié à des données.
46.	Certains types d'accréditation doivent être appliqués aux requérants d'accès sécurisé : • Lorsque les requérants accrédités recherchent des données, leur objectif doit être déclaré à chaque fois qu'une demande est faite. • Différentes conditions peuvent être appliquées à différents objectifs. • Si les requérants accrédités enfreignent les conditions établies, des pénalités doivent être appliquées.
47.	Afin de hausser la norme de protection des données d'enregistrement de gTLD, toutes les requêtes/réponses du RDS doivent faire usage d'un cryptage de message couramment disponible et de mesures d'authentification afin de protéger la confidentialité et l'intégrité des données en transit.
48.	Pour répondre aux besoins des utilisateurs authentifiés du RDS ayant des objectifs admissibles, le RDS doit fournir un service de requête inverse qui recherche des éléments de données publics et sécurisés pour une valeur spécifique et retourner une liste de tous les noms de domaine qui référencent cette valeur.
49.	Pour répondre aux besoins des utilisateurs authentifiés du RDS ayant des objectifs admissibles, le RDS doit fournir un service WhoWas qui retourne des instantanés d'éléments de données publics et sécurisés pour des noms de domaine spécifiés, limités aux données historiques à disposition du RDS.
50.	Le RDS doit soutenir les services novateurs qui font usage d'éléments de données du RDS, comme suit. • Les parties tierces doivent pouvoir fournir des services novateurs

Nº.	Principes d'accès aux données
	existants et futurs - y compris les requêtes inverses et le WhoWas - utilisant des éléments de données publics et respectant les conditions d'utilisation des données du RDS. • Dans le cas où des tiers offriraient des services novateurs impliquant des éléments de données sécurisés, ces tiers doivent être accrédités et respecter les conditions d'utilisation des données du RDS.
51.	Toutes les divulgations d'éléments de données sécurisés doivent se faire via des méthodes d'accès du RDS définies (y compris celles décrites ci-dessus). L'ensemble complet de données RDS pour tous les gTLD (ou l'ensemble complet de données du registre pour un gTLD) ne doit pas être exporté en vrac pour un accès non contrôlé.
52.	Les divulgations peuvent avoir lieu via un affichage interactif et d'autres méthodes d'accès au RDS. • Pour faciliter la recherche des données et accéder de manière cohérente, un point d'accès central (par exemple, un portail Web) doit être proposé. • L'accès sécurisé à des données publiques doit être disponible pour tous les requérants, grâce à une méthode d'interrogation anonyme (au moins à travers une page Web sécurisée). • L'accès sécurisé à des données sécurisées doit être soutenu via Web sécurisé ou d'autres méthodes et formats d'accès (par exemple, réponses xml, SMS, courriel), en fonction du requérant authentifié et de l'objectif poursuivi. • Les requérants doivent être en mesure d'obtenir du RDS des informations fiables en temps réel, si nécessaire. • Le RDS doit être apte à accueillir une automatisation des quêtes à grande échelle et ce pour divers cas d'utilisation et objectifs admissibles.
53.	Pour avoir une portée vraiment mondiale, le RDS doit être apte à afficher des données d'enregistrement en plusieurs langues, écritures et jeux de caractères, y compris les noms de domaine internationalisés (IDN).
54.	Le RDS devrait soutenir toutes les politiques futures de translittération

Nº.	Principes d'accès aux données
	définies par la GNSO pour les gTLD.
55.	Le RDS devrait permettre une collecte et un affichage des éléments de données d'enregistrement dans les langues locales.

Illustration de l'accès à des données publiques

Tel que dépeint dans la figure suivante, les éléments de données publics peuvent toujours être demandés à partir du RDS par n'importe qui, avec ou sans authentification. Se référer à l'annexe E pour une illustration plus détaillée des éléments de données retournés suite à une demande de données publiques non authentifiée.

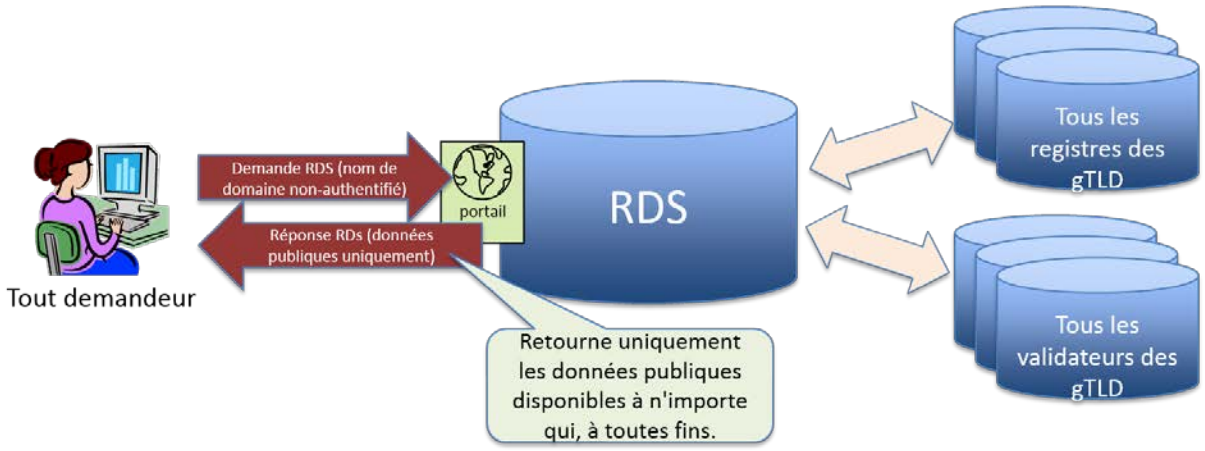


Figure 6. Accès non authentifié à des données d'enregistrement publiques via le RDS

L'annexe I comprend aussi des organigrammes et un exemple de cas d'utilisation pour illustrer les étapes impliquées dans l'accès aux éléments de données pertinents.

Illustration de l'accès à des données sécurisées

Tel que dépeint dans la figure suivante, les éléments de données sécurisés peuvent également être demandés via le RDS. Pour ce faire, les requérants doivent d'abord être accrédités. Ensuite, les requérants peuvent soumettre leurs requêtes authentifiées en demandant les éléments de données pour un objectif énoncé. Se référer à l'annexe E pour une illustration plus détaillée des éléments de données retournés suite à une requête de données sécurisées authentifiée.

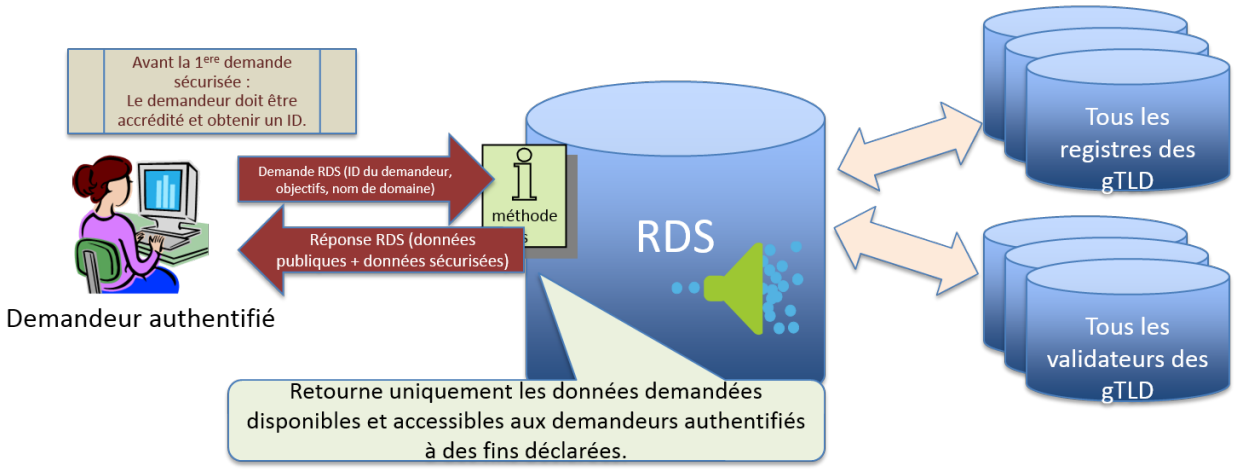


Figure 7. Accès à des données d'enregistrement sécurisées via le RDS

Protocoles techniques et méthodes d'accès

L'EWG a examiné si les protocoles techniques déployés dans le système d'enregistrement de domaines actuel (comme le protocole EPP[14]), et en cours de développement à l'IETF (comme par le groupe de travail WEIRD), pourrait soutenir les caractéristiques de conception recommandées par l'EWG. Le groupe WEIRD est près de finaliser une nouvelle norme désignée Protocole d'accès à des données d'enregistrement (RDAP). Le fait d'adopter ces protocoles dans le modèle recommandé par l'EWG peut résulter en des coûts de transition plus réduits pour chacune des parties concernées.

L'EWG a analysé si le protocole EPP pouvait soutenir chaque élément de donnée inclus dans le RDS recommandé et si le RDAP pouvait soutenir les principes recommandés par l'EWG pour les identifiants d'accès. L'analyse de l'EWG suggère que les deux protocoles EPP et RDAP peuvent être utilisés par le RDS, quelque soit le modèle alternatif choisi. Toutefois, ce faire peut nécessiter quelques extensions, ajouts ou une utilisation de « remarques » du RDAP. Une évaluation détaillée de chacun de ces protocoles est comprise à l'annexe G.

c. Principes d'accréditation d'utilisateur du RDS

Tel que noté dans la section III Objectifs, certains objectifs nécessitent un accès à tous les éléments sécurisés ou à un sous-ensemble approuvé d'éléments de données sécurisés. Tel que noté dans la section IV(b), Principe #46, tout objectif nécessitant un accès à des données sécurisées nécessite une accréditation de l'utilisateur. Toutefois,

[14] Voir EPP : norme 69, RFC 5730 - 5734

l'accréditation de l'utilisateur n'implique pas un accès illimité à des données sécurisées. Tout accès doit être basé sur un objectif, retournant uniquement des éléments de données permis pour l'objectif énoncé.

L'EWG recommande que pour chaque communauté d'utilisateurs du RDS identifiée dans la section III souhaitant un accès à des données sécurisées pour des objectifs admissibles, les experts de la communauté soient consultés pour confirmer les objectifs des données d'enregistrement identifiés par l'EWG, les éléments de données qui doivent être accessibles pour cet objectif et les agents d'accréditation éventuels des utilisateurs du RDS.

Il est probable que plusieurs organisations passent des contrats avec l'ICANN pour servir d'organismes d'accréditation des utilisateurs du RDS. Les organismes d'accréditation des utilisateurs du RDS doivent être guidés par un ensemble de principes communs mais il est probable que les mises en œuvre soient différentes selon la communauté d'utilisateurs du RDS. Par exemple :

Scénario #1 : L'organisme d'accréditation est différent de l'opérateur d'accréditation ; l'organisme approuve les utilisateurs mais une tierce partie, l'opérateur, gère l'accès au RDS des utilisateurs accrédités

Pour une communauté d'utilisateurs du RDS comme les détenteurs de marques de commerce, une organisation du secteur pourrait assumer la responsabilité d'accréditer ses propres membres qui souhaitent accéder à des données sécurisées pour des objectifs admissibles. L'organisme d'accréditation peut ne jouer aucun rôle dans la gestion des comptes des utilisateurs ou l'authentification des demandes d'accès envoyées au RDS. Plutôt, l'organisme d'accréditation établit des règles qui régissent les membres, des conditions de service et des processus de demande et de mise en application, etc. pour une communauté d'utilisateurs du RDS donnée. L'organisme d'accréditation peut alors passer un contrat avec un tiers, un opérateur d'accréditation pour créer et gérer les comptes d'utilisateurs du RDS, émettre des identifiants d'accès au RDS, authentifier les demandes d'accès au RDS et fournir un traitement en cas d'abus de premier niveau, y compris la suspension provisoire d'un compte. L'opérateur d'accréditation met simplement en œuvre et en application les règles d'accès au RDS établies par l'organisme d'accréditation pour une communauté donnée ; tous appels en cas de suspension de compte ou autres litiges seraient transmis à l'organisme d'accréditation.

Scénario #2 : Organisme d'accréditation combiné à un opérateur d'accréditation, qui transmet les demandes d'accès au RDS authentifiées au RDS

Pour une communauté d'utilisateurs du RDS comme OpSec, une organisation du secteur pourrait assumer la responsabilité d'accréditer ses propres membres via un processus d'accréditation (approuvé) qu'elle utilise déjà pour accorder aux utilisateurs un accès à d'autres systèmes. Dans cet exemple, l'organisation sert en même temps d'organisme d'accréditation et d'opérateur d'accréditation, tirant parti d'un système existant déjà utilisé par ses propres membres pour authentifier et transmettre au RDS des demandes d'accès sécurisé pour des objectifs admissibles. Dans ce cas, l'utilisateur du RDS est responsable de la conformité aux conditions et l'organisation du secteur doit établir un processus qui traite les abus d'accès, les suspensions, etc. s'appliquant aux accès au RDS d'un utilisateur spécifique.

Scénario #3 : Organisme d'accréditation combiné à un opérateur d'accréditation, servant d'intermédiaire pour les demandes d'accès au RDS pour le compte de ses membres (c'-à-d. le modèle Interpol)

Pour une communauté d'utilisateurs du RDS comme les représentants de la loi, une organisation reconnue, crédible, pourrait assumer la responsabilité d'accréditer ses propres membres via un processus d'accréditation (approuvé) qu'elle utilise déjà pour accorder aux utilisateurs un accès à d'autres systèmes. Dans cet exemple, l'organisation sert en même temps d'organisme d'accréditation et d'opérateur d'accréditation, tirant parti d'un système existant déjà utilisé par ses propres membres pour authentifier et servir d'intermédiaire pour les demandes d'accès sécurisé au RDS pour des objectifs admissibles. Dans ce cas, l'organisation est considérée comme étant l'utilisateur du RDS et assume la responsabilité des actions de ses membres concernant les demandes exprimées et conformes aux conditions. Le RDS peut ne pas être au courant des activités spécifiques des utilisateurs mais l'organisation doit établir un processus pour traiter les abus d'accès, les suspensions, etc., d'une manière qui permette à l'organisation de vérifier des accès d'utilisateurs spécifiques et de détecter les abus.

Pour permettre un accès accrédité d'utilisateur du RDS à des éléments de données sécurisés pour des objectifs admissibles, l'EWG recommande les principes d'accréditation d'utilisateur du RDS suivants.

Nº.	Principes d'accréditation d'utilisateur du RDS
56.	L'accès non accrédité, non authentifié à des données non sécurisées (c'-à-d. publiques) doit être possible en temps réel.
57.	L'accréditation d'utilisateurs du RDS pour un accès à des données du RDS ne doit pas nécessairement avoir lieu en temps réel pour tous les cas d'utilisation et/ou les requérants.
58.	Le RDS doit uniquement appliquer le « schéma d'accréditation » minimum nécessaire pour fournir un accès d'utilisateur du RDS à des éléments de

Nº.	Principes d'accréditation d'utilisateur du RDS
	données sécurisés pour l'objectif énoncé.[15]
59.	Il ne doit pas y avoir d'exigence de « pré-approbation » ou de fourniture d'identifiants pour chaque utilisateur potentiel du RDS. Un processus de demande et de conformité peut être créé pour chaque « type » d'utilisateur accrédité du RDS (c'-à-d. communauté d'utilisateurs du RDS).
60.	L'accréditation pour les utilisateurs du RDS qui souhaitent un accès à des données pour des objectifs admissibles pourrait être accordée de trois manières. • Aucune (c'-à-d. accès non authentifié à des données publiques uniquement, comme ci-dessus). • Auto-accréditation par la personne/l'entité demandant les données, comme un système où l'utilisateur déclare simplement qui il est, les données requises et pourquoi, et obtient ensuite l'accès à ce niveau de données. Par exemple, ceci pourrait s'appliquer à des titulaires de noms de domaine qui ont besoin d'accéder aux données de leur propre nom de domaine pour un contrôle du nom de domaine ; leur attestation est liée à l'enregistrement du nom de domaine et ceci les qualifie pour obtenir un identifiant et un accès à ces informations dans le RDS. • L'accréditation par une tierce partie crédible (c'-à-d. organisme d'accréditation d'utilisateur du RDS, voir principe #64 ci-dessous).
61.	Dans la mesure du possible, tout processus d'accréditation du RDS par une tierce partie devrait tirer parti des processus d'accréditation existants dans chaque communauté d'utilisateurs du RDS identifiée dans la section III comme pouvant avoir besoin d'identifiants.
62.	Ces processus d'accréditation par une tierce partie doivent être contrôlés par une autorité responsable de la mise en œuvre et de l'application de la politique d'accréditation d'utilisateurs du RDS (par exemple, l'ICANN, un panel multipartite) et révisés de manière périodique.
63.	Toute organisation servant d'organisme d'accréditation d'utilisateurs du RDS doit avoir signé un accord avec l'ICANN et/ou avec le fournisseur du RDS pour offrir de tels processus d'accréditation selon des directives convenues et établir un cadre pour permettre un processus approprié, responsabilité, sécurité, accès équitable et respect de la loi en vigueur.

[15] Par exemple, cette accréditation n'a pas besoin d'exiger des déclarations sur l'honneur multifactorielles ou de servir comme système miracle pour obtenir la plupart des types de données.

Nº.	Principes d'accréditation d'utilisateur du RDS
64.	Les accréditeurs peuvent assumer l'une ou les deux responsabilités suivantes. • Un organisme d'accréditation d'utilisateurs du RDS peut définir et gérer une communauté d'utilisateurs, y compris établir des critères d'adhésion, des exigences pour la qualification et définir et appliquer ses propres conditions d'adhésion. • Un opérateur d'accréditation d'utilisateurs du RDS peut offrir une plate-forme utilisée par les organismes d'accréditation, fournissant des fonctions telles que création de compte d'utilisateur, attribution d'identifiants, suspension et révocation, gestion de compte d'utilisateur à vie et autres processus y liés comme le traitement de litiges et autres. Un accréditeur donné peut, sans y être obligé, assumer les deux responsabilités.
65.	Les accréditeurs qui souhaitent participer au traitement des demandes au RDS pour des données pour le compte de leurs membres peuvent le faire de manières : • Un accréditeur peut fournir un accès au RDS en tant qu'intermédiaire via son propre système d'authentification et assumer la pleine responsabilité quant à la conformité de l'usage. Bien que l'accréditeur soit tenu responsable en cas d'abus, les demandes transmises par le biais des accréditeurs de cette manière doivent être authentifiées de sorte à permettre le contrôle et la résolution de plaintes à propos d'abus liées à l'accès d'un utilisateur particulier. • Un accréditeur peut fournir un accès au RDS via son propre système d'authentification mais simplement relayer les demandes authentifiées au RDS. Les demandes transmises par le biais de l'accréditeur de cette manière doivent uniquement identifier l'utilisateur du RDS, qui est responsable de la conformité de l'usage et qui sera tenu directement responsable en cas d'abus.
66.	Tel que défini dans la section IV(b), Principe #50, le RDS doit fournir un accès en temps réel aux requérants accrédités via de multiples méthodes. Les demandes peuvent être authentifiées par l'opérateur d'accréditation approprié et les identifiants d'accès au RDS délivrés durant l'accréditation doivent pouvoir être utilisés pour toutes les méthodes d'accès définies.[16]

[16] Les interfaces d'authentification doivent être définies durant la mise en œuvre. Par exemple, pour certaines méthodes d'identifiants, le RDS peut utiliser un cadre standard tel que le langage de balisage d'assertion de sécurité (SAML(pour permettre l'authentification par l'opérateur d'accréditation qui a émis cet identifiant.

Nº.	Principes d'accréditation d'utilisateur du RDS
67.	Les bonnes pratiques peuvent être définies pour la gestion d'identifiants ; les accréditeurs doivent être tenus d'adhérer aux bonnes pratiques.
68.	Le RDS doit exiger des identifiants individuels pour un accès authentifié.
69.	L'accès authentifié au RDS ne doit pas être transitif (c'-à-d. un utilisateur authentifié du RDS ne devra pas partager des données sécurisées avec d'autres en dehors de son accréditation).
70.	Un processus pour une divulgation responsable des données sécurisées pour desservir l'objectif initial pour lequel elles ont été demandées doit être créé et appliqué. (par exemple, permettant à un détenteur de PI enquêtant sur une violation de marque de commerce de déposer une plainte UDRP, permettant à un utilisateur OpSec enquêtant sur une éventuelle activité criminelle de notifier les représentants de la loi).
71.	Une organisation cherchant à accéder aux données du RDS pourrait déposer une demande pour une accréditation d'utilisateur du RDS et couvrir toutes les personnes utilisant le RDS et appartenant à cette organisation au moyen de cette accréditation unique.[17] Une telle organisation est responsable de la gestion de l'accès accrédité en son sein. Une mauvaise utilisation du système par les membres d'une organisation utilisatrice du RDS accréditée conduirait à une pénalisation de l'organisation dans son ensemble.
72.	Un seul utilisateur du RDS remplissant des rôles différents peut avoir de multiples identifiants afin d'accéder à différents types de données pour des objectifs différents. Toutefois, il est grandement souhaitable du point de vue commodité de fournir un seul identifiant par utilisateur de RDS qui pourrait être utilisé pour de multiples objectifs, dans la mesure où chaque objectif est énoncé par accès tel que défini dans la section IV(b).
73.	Des audits et des analyses de données doivent être utilisées pour identifier l'abus du système et des identifiants d'accès.
74.	Un processus d'appel doit être défini pour permettre aux utilisateurs du RDS de réfuter les allégations d'abus lorsqu'ils essaient de réactiver/rétablir des identifiants d'accès au RDS.
75.	Chaque titulaire de nom de domaine doit recevoir un identifiant pour pouvoir examiner ses propres données de contact entreposées par le RDS concernant les noms de domaine y enregistrés. (Voir section III, objectif de contrôle de nom de domaine.)
76.	Un processus pour ajouter des accréditeurs d'utilisateurs du RDS

[17] Il appartient à l'organisation de garantir l'intégrité de tous identifiants émis pour accéder au RDS.

Nº.	Principes d'accréditation d'utilisateur du RDS
	supplémentaires qui complète des processus actuels ou offre de nouvelles manières innovatrices de fournir une accréditation d'utilisateur du RDS pour des objectifs approuvés doit être établi. De tels accréditeurs d'utilisateurs du RDS doivent satisfaire les exigences minimum décrites dans les principes énumérés ici.

d. Résumé des principaux avantages en matière de responsabilité

Le fait d'incorporer un accès accrédité à des éléments de données sécurisés fait partie intégrante du RDS de nouvelle génération ; ceci améliorera la responsabilité en exigeant de ceux qui accèdent à des données plus sensibles de s'identifier et d'énoncer l'objectif poursuivi. Plus particulièrement, les avantages qui résulteraient de l'adoption des principes d'accès et éléments de données recommandés par l'EWG comprennent ce qui suit.

- Établir une collecte de données et un paradigme de divulgation orientés sur les objectifs pour promouvoir la responsabilité quant aux entités qui utilisent les données d'enregistrement pour des objectifs admissibles.
- Fournir un cadre de soutien pour se conformer aux lois de protection des données dans les diverses juridictions.
- Établir une méthode qui fournisse une responsabilité des personnes accédant aux données pour divers objectifs. Ceci soutient aussi les exigences de protection des données/confidentialité dans les diverses juridictions et garantit un équilibre de responsabilité entre ceux qui doivent fournir des données exactes et ceux qui les utilisent pour des objectifs approuvés. Ceci résout une inégalité fondamentale par rapport au système WHOIS où les requérants de données n'ont aucune responsabilité en matière d'accès et d'utilisation des données de contact.
- Fournir aux titulaires des noms de domaine et aux contacts une meilleure compréhension des objectifs dans lesquels les données d'enregistrement sont collectées et un contrôle discrétionnaire plus important sur la qualification des informations personnelles comme publiques ou sécurisées.
- Satisfaire les besoins universels en matière de données d'enregistrement par un ensemble de données publiques de base tout en réduisant les données qui sont publiques par défaut et en authentifiant ceux qui accèdent aux données sécurisées.
- Augmenter l'exactitude des données, compte tenu de la protection des éléments de données sensibles et leur non divulgation publique, conduisant à un partage plus probable de données plus exactes par les titulaires de noms de domaine et les PBC.

A l'exception de l'utilisation malveillante, lorsque les données sont protégées contre une publication générale, les parties faisant l'objet de ces données fourniront souvent des informations plus exactes afin d'obtenir tous les avantages associés puisque le risque fondamental perçu est réduit.

- Améliorer globalement la résilience et l'efficacité de la communication pour les utilisateurs et les titulaires des noms de domaine du RDS en incorporant de nouveaux éléments de données facultatifs pour faciliter le contact via des méthodes de communication nouvelles ou alternatives.
- Soutenir les requêtes inverses et WhoWas par le biais d'un portail central pour permettre des recherches dans tous les enregistrements de gTLD, par des utilisateurs du RDS accrédités et uniquement pour des objectifs admissibles.
- Permettre des capacités d'accès renforcées pour améliorer l'efficacité globale du « système ».
- Fournir un accès, non authentifié à des données publics et avec identifiant à des données sécurisées, pour éliminer le méli-mélo des capacités d'accès, les niveaux de service et les formats dans les réponses actuelles du WHOIS sur les gTLD et permettre une mise en œuvre facile des requêtes automatisées du RDS via une norme unique.
- Fournir un service de qualité et un accès fiable, permettant la retraite des diverses mesures anti-abus réparties à travers l'écosystème.

Pour obtenir ces avantages, il sera extrêmement important d'éduquer les utilisateurs du RDS en matière d'objectifs admissibles et d'utilisations appropriées des données recueillies du RDS. Trouver des accréditeurs disposés à assumer la responsabilité pour approuver l'accès au RDS de la part des membres de leur communauté pourrait être difficile. Au départ, les utilisateurs pourraient avoir des difficultés à identifier l'accréditeur approprié, notamment concernant les utilisateurs qui interagissent avec le RDS pour plusieurs objectifs. Les requêtes automatisées du RDS nécessiteront aussi des outils de mise à jour. Toutefois, ces investissements initiaux nécessaires pour établir un accès orienté sur l'objectif poseront des fondations solides pour que les utilisateurs du RDS soient responsables dans le cadre de l'utilisation des données d'enregistrement.

V. Améliorer la qualité des données

L'EWG recommande une validation plus solide des données des titulaires de noms de domaine que celle fournie dans le système actuel WHOIS ou des améliorations qui peuvent être réalisées à travers une vaste mise en œuvre du 2013 RAA. D'abord, la mise à disposition de contacts orientés sur les objectifs par les titulaires de noms de domaine

devrait mener à des améliorations significatives de l'accessibilité à des contacts appropriés à des fins diverses et motive les titulaires de noms de domaine quant à fournir des informations précises pour ces rôles. Deuxièmement, l'accès sécurisé à des éléments de données plus sensibles, encouragera moins les titulaires à fournir des données inexactes, et renforcera leur responsabilité quant à assurer l'exactitude des données.

Pour réaliser ces objectifs, l'EWG recommande deux améliorations indépendantes mais liées :

- Le RDS doit appliquer une validation standard à toutes les données d'enregistrement de gTLD. En plus des vérifications périodiques, la validation aurait lieu au moment de la collecte, avec une option de pré-validation de blocs de données de contact pour réutilisation dans les enregistrements multiples de noms de domaine.
- L'écosystème du RDS doit inclure un annuaire de contacts pré-validé, séparé sur le plan conceptuel de l'annuaire des noms de domaine, afin de promouvoir la qualité et l'utilité nouvelle des éléments de données utilisés pour contacter les titulaires de noms de domaine et les personnes ou les organisations qui peuvent être désignées par les titulaires comme des PBC à diverses fins associées à l'enregistrement d'un nom de domaine, et afin de prévenir les usages frauduleux des données personnelles.

Les principes et les processus pertinents à ces recommandations sont décrits en détail ci-dessous. Pour maximiser les avantages, l'EWG recommande les deux améliorations mais note que la création d'un annuaire de contacts est possible sans une validation accrue et vice versa.

a. Exactitude des données et principes de validation

La pré-validation des informations du titulaire du nom de domaine ou autre contact est souhaitée pour :

- Augmenter la précision des informations de contact en utilisant la pré-validation pour vérifier les données avant l'usage concernant un nouveau nom de domaine et pour promouvoir des données cohérentes à travers tous les enregistrements (réduit l'erreur et la fraude) :
- Éviter le besoin de valider les données de contact du titulaire du nom de domaine ou des PBC chaque fois qu'un titulaire de nom de domaine enregistre un nouveau nom de domaine en effectuant la validation une fois et en réutilisant

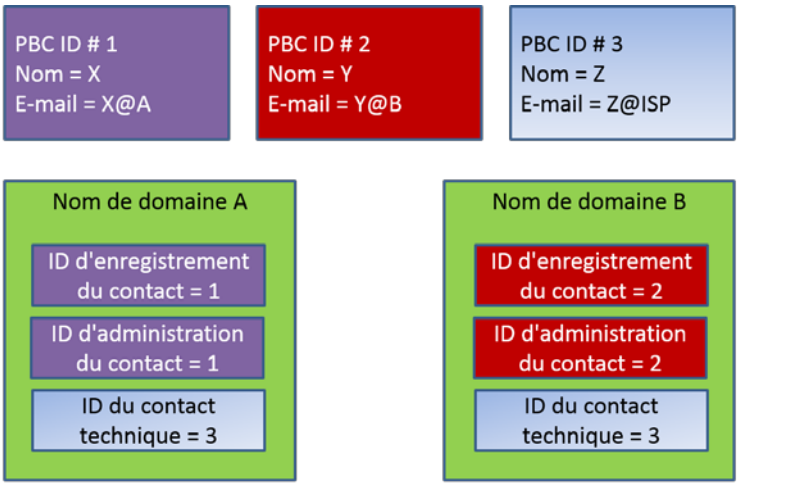
ce bloc de données de contact pour plusieurs enregistrements de noms de domaine (simplifie le processus et réduit les exigences de travail) ; et

- Éviter le retard dans le traitement de l'enregistrement du domaine, puisque la validation doit avoir lieu au moment de l'enregistrement.

Plusieurs fournisseurs de services, représentants légaux et autres tiers sont souvent les points de contact primaires pour plusieurs rôles (par ex. technique, facturation, abus, action en justice) concernant des domaines enregistrés par une grande variété de titulaires de noms de domaine (souvent des centaines ou des centaines de milliers de domaines).

Pour permettre une plus grande précision dans un espace diversifié et une facilité d'utilisation de tels contacts, il est souhaitable de fournir des mécanismes permettant un usage facile de ces contacts par de multiples titulaires de noms de domaine ; par ex. une entreprise d'hébergement Web fournissant son ID NOC unique pour les contacts « technique » et en «cas d'abus » pour les domaines contrôlés par ses clients. De plus, lorsqu'une telle entité a besoin d'actualiser ses informations de contact pour refléter une nouvelle adresse, un nouveau numéro de téléphone ou une fusion/acquisition, il devrait être facile d'actualiser ces informations en un seul endroit et que ceci se reflète dans tous les domaines associés à cet ensemble de données de contact (désigné par un identifiant unique).

La figure suivante présente un paradigme dans lequel des contacts basés sur les objectifs (PBC) pourraient être créés, associés à des identifiants uniques (ID PBC) et puis réutilisés dans des enregistrements de noms de domaine multiples. Tel que détaillé dans la section III, les PBC ne représentent pas nécessairement des personnes mais plutôt des points de contact publiés explicitement créés par les détenteurs des contacts et visant à permettre la communication à des fins liées au DNS.



Mises à jour faites aux ID du PBC #3 automatiquement reflétées dans les données d'enregistrement pour les noms de domaine A et B

Nº.	Principes pour les ID des contacts et données y associées
77.	La gestion des contacts doit être faisable séparément de la gestion des noms de domaine, permettant une transférabilité et une responsabilité séparées des noms de domaine et contrôlées par les individus ou les entités inscrites sous ces contacts.
78.	Les contacts doivent être gérés en utilisant des validateurs qui gèrent les bases de données de contacts, appliquent les régimes de validation et maintiennent les informations au niveau de validité pour le contact et ses éléments de données (accessibles via le RDS).[18]
79.	Les enregistrements de noms de domaine peuvent être associés à des ID de contacts désignés par leurs titulaires et approuvés par ces contacts désignés pour différents objectifs associés à un nom de domaine.
80.	De tels contacts doivent contenir des éléments de données obligatoires valides. Des politiques et une supervision seront nécessaires pour gérer ces processus afin de s'assurer que les ID de contact ne soient pas utilisés sans l'autorisation du contact et satisfassent les normes minimum.
81.	La gestion des changements et l'autorisation d'utilisation des informations de contact sont contrôlées par le détenteur du contact et concernent tous les domaines associés à ce contact. Des processus et des politiques pour assurer la

[18] NOTE : Les bureaux d'enregistrement peuvent et sont probablement à même de devenir des validateurs accrédités afin de fournir des services de validation aux contacts associés aux noms de domaine qu'ils enregistrent.

Nº.	Principes pour les ID des contacts et données y associées
	mise en œuvre précise, authentique et opportune des changements souhaités sans surcharger les PBC ou les titulaires de noms de domaine doivent être élaborés afin de soutenir ce nouveau paradigme.
82.	Chaque bloc individuel de données de contact doit avoir un ID de contact qui identifie de façon unique le validateur et le détenteur du contact pour permettre la récupération et l'actualisation des données de contact associées. Cet ID de contact doit être publié dans tout affichage public de données du RDS.

b. Processus de pré-validation

Pour parer à ces besoins, le processus suivant de pré-validation est recommandé :

a) Chaque candidat soumet ses données de contact via un validateur de son choix (par ex. bureau d'enregistrement, registre, tierce partie accréditée gestionnaire de contact).

b) La validation syntaxique et opérationnelle (selon le SAC-058) est effectuée par le validateur.

c) **FACULTATIF** : La validation de l'identité peut être effectuée par les validateurs, en utilisant des entités telles que les bureaux de poste, les gestionnaires de ccTLD, les compagnies de téléphone, l'administration fiscale, etc. *Il faudrait noter que les contacts ayant satisfait les normes facultatives de validation de l'identité peuvent être désignés en tant que tels dans leur statut afin de renforcer la confiance de l'utilisateur, ce qui facilite le commerce en ligne. Il faudrait également noter que de tels services de plus-value seraient probablement associés à un coût qui serait assumé par l'entité demandant ce niveau supplémentaire de validation.*

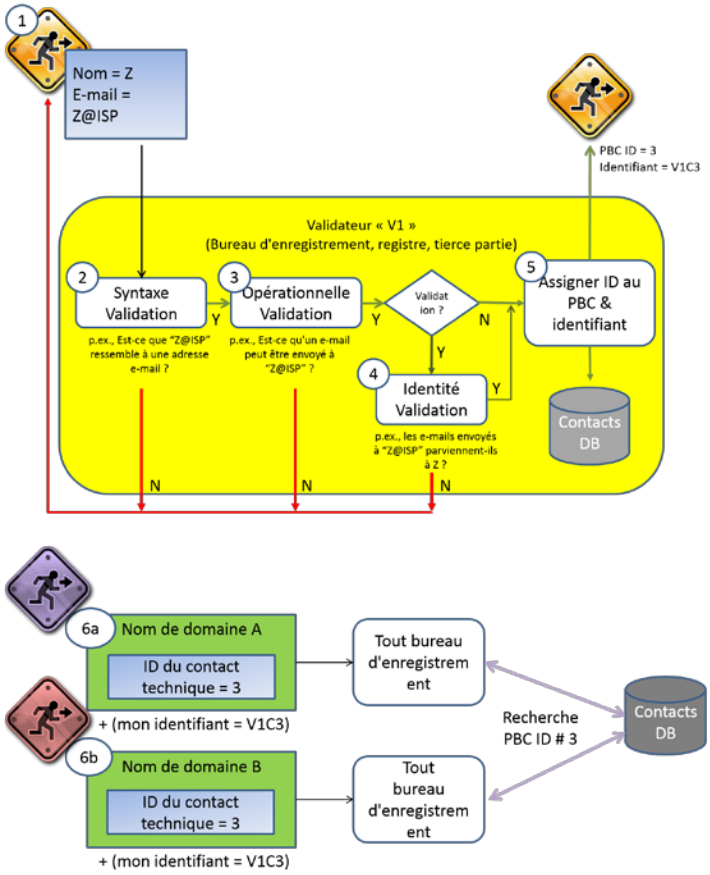
d) Après une validation syntaxique réussie et toute validation opérationnelle requise, un identifiant unique est émis au bloc de données de contact (contact) par le validateur, identifiant autant le validateur que le contact pour permettre la récupération et l'actualisation subséquentes.

e) Le validateur entrepose les données de contact dans sa propre base de données, émet des identifiants (selon le cas, pour permettre des actualisations futures du contact) et transmet l'identifiant unique au candidat (désormais dénommé détenteur du contact).

f) Le détenteur du contact fournit cet ID de contact aux titulaires de noms de domaine qui pourraient s'adresser alors à tout bureau d'enregistrement, utilisant cet identifiant unique, pour enregistrer leurs noms de domaine en utilisant les ID des

contacts comme contacts basés sur les objectifs (c.-à-d. PBC). *Tel que défini dans la section III, un processus d'autorisation doit être mis en place pour s'assurer que le titulaire du nom de domaine et son contact désigné sont d'accord sur les objectifs que ce PBC va accepter pour chaque nom de domaine.*

g) Des ID de contact validés peuvent être désignés comme PBC pour un nom de domaine (par ex. titulaire, technique, admin, commercial, en cas d'abus, fournisseur PP) suivant les principes pour les contacts basés sur objectifs définis dans la section III(e).



Il faudrait noter que chaque validateur maintient sa propre base de données de contacts. Ces données doivent aussi être fournies au RDS, mais ce mécanisme dépend du modèle de RDS tel que décrit dans la section VII. Par exemple, dans le modèle synchronisé, les ajouts et les actualisations de données de contact peuvent se faire par EPP au RDS. Dans le modèle fédéré, les données de contact peuvent être tirées par le RDS en temps réel via RDAP.

c. Exactitude, audit et processus de restauration

Les processus suivants sont recommandés pour assurer une exactitude continue des données d'enregistrement et une restauration des données d'enregistrement inexactes :

a) **Auto-correction** : Le détenteur du contact utilise le validateur pour corriger / actualiser ses données utilisant les identifiants précédemment émis. Les informations passent automatiquement à tous les domaines utilisant ce contact particulier (tel que désigné par l'ID de contact unique).

b) **Processus suivi** : Les validateurs effectuent des validations d'identité périodiques opérationnelles et facultatives des jeux de contact gérés par le biais de leur service. *Note : De telles procédures de validation ne devraient pas être trop pesantes mais pourraient être reflétées dans les statuts publiés pour un contact (par ex. le contact est valide du point de vue opérationnel à compter du 1 janvier 2016).*

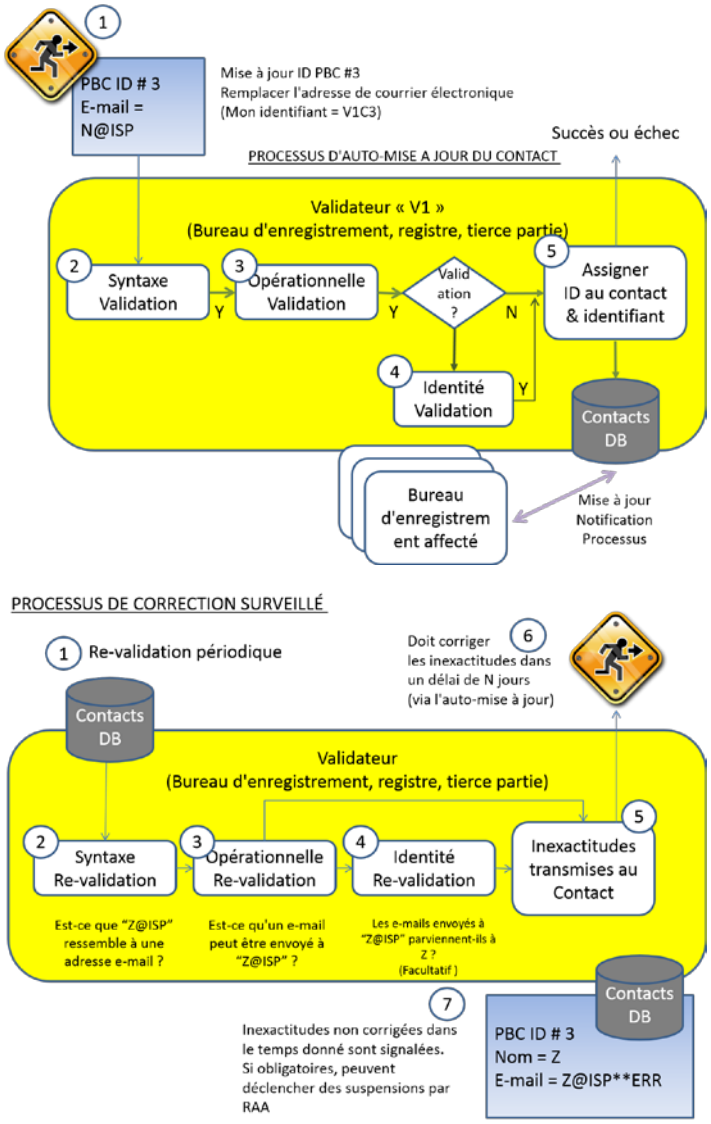
c) Les validateurs signalent toutes données inexactes détectées au détenteur du contact, lui accordant une période de temps spécifique (par exemple 14 jours) pour corriger l'inexactitude. Les titulaires de noms de domaine, les registres et les bureaux d'enregistrement des domaines touchés peuvent être notifiés. Le détenteur du contact utilise le validateur choisi au préalable pour corriger l'exactitude en utilisant ses identifiants précédemment émis.

d) Si les données d'enregistrement demeurent inexactes après l'échéance, les données sont marquées comme étant inexactes. Si les données marquées sont obligatoires pour un PBC faisant référence à cet ID de contact, les domaines associés sont alors placés dans un processus de restauration qui notifierait le titulaire du nom de domaine concernant l'inexactitude et lui permettrait de la corriger dans une période de temps spécifiée dans le RAA. Ne pas corriger une telle inexactitude pourrait conduire à des pénalisations du nom de domaine qui peuvent inclure une suspension ou une suppression selon le RAA en vigueur.

e) Lorsque les données marquées sont remplacées par des données valides, toutes les pénalisations affectant le nom de domaine sont levées.

f) Dans le cas de rapports d'exactitude soumis du département de conformité de l'ICANN, le validateur sera notifié pour répéter la validation syntaxique et opérationnelle. Si la revalidation réussit, la partie ayant soumis le rapport d'exactitude peut entreprendre d'autres actions appropriées à sa situation (par ex. déposer une plainte UDRP ou soumettre une requête de divulgation). Si la revalidation échoue, les titulaires de tous les noms de domaine utilisant cet ID de

contact inexact doivent être notifiés et suivre le processus de restauration normal décrit ci-dessus.



d. Cadre opérationnel pour les ID de contact

Le cadre suivant est recommandé pour gérer les ID de contact et les associer à des informations d'enregistrement :

a) Les ID de contact doivent être uniques quelque soit le validateur pour assurer la transférabilité et fournir des correspondances définitives entre les noms de domaine et les informations d'annuaire nécessaires.

b) Les ID de contact qui identifient autant le contact que le validateur doivent être associés à des blocs d'informations de contact discrets pour permettre la récupération et l'actualisation. Explication : un ID de contact correspond à un jeu

de données de contact qui est utilisable pour communiquer avec les contacts du nom de domaine désignés. Les informations qui ne satisfont pas cette exigence sont inutiles du point de vue opérationnel.

c) Les ID de contact doivent être émis par des validateurs accrédités. Toute entité peut demander à devenir un validateur, sous réserve de critères analogues à ceux actuellement utilisés pour accréditer les bureaux d'enregistrement. Les validateurs accrédités peuvent inclure des bureaux d'enregistrement, des registres et des tiers fournisseurs de validation. Fondements : un validateur est une fonction nécessaire pour créer une base de données de contact. Le niveau de validation peut varier selon le contact, mais le processus a besoin d'être harmonisé parmi les validateurs pour assurer l'exactitude et la responsabilité des titulaires de noms de domaine et de leurs contacts désignés.

d) Pour être associé à un nom de domaine, le titulaire du nom de domaine ou le PBC désigné doit obtenir un ID de contact.

e) Les ID de contact peuvent être attribués à de multiples rôles pour un ou plusieurs noms de domaine. Par ex., un ID de PBC donné peut être utilisé comme ID de titulaire de nom de domaine pour un domaine et comme contact technique et en cas d'abus pour d'autres domaines.

f) Les contacts peuvent être créés et modifiés à tout moment, y compris dans le cadre du processus d'enregistrement du domaine.

e. Interaction avec les validateurs

L'EWG recommande les principes suivants pour l'interaction entre les validateurs et les détenteurs de contact (c.-à-d. les parties qui créent avec succès des blocs de données de contact validées, réutilisables).

Nº.	Principes d'interaction entre les détenteurs de contact et les validateurs
83.	Pour tout ID de contact donné, un détenteur de contact peut choisir tout validateur[19].
84.	Des politiques de supervision et de responsabilité relatives à la gestion des ID de contact doivent être élaborées.
85.	Les détenteurs du contact doivent être capables de modifier les informations de

[19] Selon le principe #88, les ID de contact identifient autant le validateur que le détenteur du contact. Ceci devrait être mis en œuvre de façon à permettre la transférabilité de l'ID de contact entre les validateurs.

Nº.	Principes d'interaction entre les détenteurs de contact et les validateurs
	contact associées à un ID de contact par le biais du validateur.
86.	Les validateurs doivent utiliser l'authentification du détenteur du contact afin d'empêcher une modification non autorisée des informations de contact associées à un ID de contact.
87.	Les validateurs peuvent offrir plusieurs niveaux d'authentification de détenteur de contact, allant d'une authentification PIN de base à une authentification à deux facteurs. Les détenteurs de contact doivent être capables de choisir des fournisseurs en fonction des propositions de coût/bénéfice liées à la facilité d'utilisation, aux coûts et autres facteurs commerciaux logiques.
88.	Les validateurs doivent publier leurs politiques relatives à l'authentification d'une manière qui puisse être utilisée mondialement pour la gestion de la réputation. Ceci encouragera une meilleure exactitude et responsabilité en matière d'informations de contact inscrites.
89.	Les validateurs doivent être capables de valider les informations de contact soumises dans la langue maternelle du détenteur du contact. Ceci devrait améliorer l'exactitude des données en langue maternelle et soutenir l'extensibilité du système d'enregistrement de noms de domaine dans un environnement multilingue. Par exemple, les bureaux d'enregistrement pourraient travailler avec des validateurs dans plusieurs localités pour fournir des services de validation étendus à de grands nombres de titulaires de noms de domaine et de contacts désignés sans avoir à investir dans des outils coûteux pour valider les données dans des langues peu familières pour leur propre personnel.

f. Principes pour la validation de contact

Les données de contact peuvent être validées à trois niveaux différents : syntaxique, opérationnel et identité, selon le SAC 058. L'EWG recommande les principes suivants de niveau de validation.

Nº.	Principes pour la validation de contact
90.	Tous les éléments de données de contact associés à un ID de contact doivent être validés à un niveau syntaxique. Ceci représente un niveau de validation de base qui doit être réalisable par toute entité du secteur.
91.	Tous les éléments de données de contact obligatoires associés à un ID de contact

Nº.	Principes pour la validation de contact
	pour un objectif particulier doivent être validés du point de vue opérationnel[20] avant que cet ID de contact puisse être inclus dans les données d'enregistrement du nom de domaine pour cet objectif.
92.	Un détenteur de contact peut volontairement rechercher des niveaux de validation facultatifs plus élevés (par ex. validation d'identité facultative), assumant les coûts associés en faveur des avantages perçus (par ex. une plus grande confiance du consommateur dans les noms de domaine enregistrés par des entités à identité validée)[21].
93.	Les coûts donnés relatifs à une validation facultative d'identité, un mécanisme à bas coût pour que les détenteurs de contact économiquement défavorisés puissent obtenir une validation facultative d'identité sont souhaitables.
94.	Afin de préserver les associations et permettre la mise en place d'un processus de correction, l'ID de contact peut avoir un statut marqué « inexact » et rester dans le système.
95.	Le statut de validation de l'ID de contact doit être suivi et publié le cas échéant lors de l'accès à des informations du RDS, avec la dernière date à laquelle le statut de validation a été déterminé.
96.	Les tiers peuvent déposer des rapports d'inexactitude pour contester un statut de validation d'un ID de contact, tel que décrit dans la section V(c), déclenchant un processus de restauration standard qui peut résulter en un marquage de l'ID de contact comme « inexact » et en d'autres conséquences pour les noms de domaine utilisation cet ID de contact comme PBC.
97.	Les domaines actifs ne peuvent pas avoir un contact obligatoire dont le statut est « inexact » sans une restauration de quelque sorte. Le schéma peut toutefois être défini ailleurs.
98.	Un niveau minimum de validation inter-champs doit être vérifié pour tous les

[20] Se référer au SAC 058 et au *résumé des résultats de l'enquête dur la validation/vérification des données du WHOIS pour les ccTLD* pour des façons possibles de mettre en œuvre la validation opérationnelle et les pratiques de ccTLD existantes.

[21] Par exemple, une validation facultative d'identité pourrait être un ajout séparément facturé ou inclue dans les paquets d'enregistrement de noms de domaine ou offerte comme motivation aux gros clients. Se référer au document *RFI sur les systèmes de validation et de vérification de données de contact* pour des exemples de services commerciaux qui effectuent une telle validation.

Nº.	Principes pour la validation de contact
	éléments de données de contact associés aux ID de contact lorsque la validation inter-champs est applicable (par ex. adresse physique).
99.	Une revalidation des données de contact doit être réalisée régulièrement par le validateur concerné pour s'assurer que les données sont exactes au niveau déclaré.
100.	Si le détenteur du contact fournit des éléments de données facultatifs, ces éléments doivent être au moins syntaxiquement validés. Les éléments de données facultatifs ne seraient pas validés mis à part la syntaxe sauf si le contact le demande et paze vraisemblablement tous coûts associés à une telle validation.
101.	Le niveau de validation réalisé au-delà de la validation syntaxique pour des éléments de données qui peuvent être validés du point de vue opérationnel ou (facultativement) du point de vue identité, doit être noté et conservé par le validateur. Par exemple, les éléments tels que le courriel, le numéro de téléphone et l'adresse pourraient être validés du point de vue opérationnel, alors qu'un nom ou un nom d'organisation ne pourrait pas être validé du point de vue opérationnel mais pourrait facultativement être validé du point de vue identité.
102.	En outre, le validateur doit définir et publier en tant qu'élément de donnée RDS le statut de validation global réalisé par chaque ID de contact. Par exemple, si TOUS les éléments de données obligatoires qui peuvent être validés du point de vue opérationnel passent ces vérifications, le statut de validation global du contact serait « validé du point de vue opérationnel ». si UN élément de données quelconque obligatoire qui peut être validé du point de vue opérationnel échoue, le statut de validation global du contact serait dégradé à « validé syntaxiquement ». Si TOUS les éléments de données obligatoires qui peuvent être validés du point de vue identité passent cette vérification facultative, le statut de validation global du contact serait promu à « validé du point de vue identité ». Pour promouvoir l'exactitude et la communication efficace, ce statut de validation global doit être mis à disposition des utilisateurs du RDS comme un nouvel élément de données consolidé par contact.[22]

[22] L'EWG a aussi envisagé la publication d'éléments de données du RDS pour transmettre le statut de validation individuel de chaque élément de données de contact individuel (par ex. statut de courriel PBC = validé du point de vue opérationnel, statut de nom PBC = validé du point de vue identité). Publier le statut de validation ainsi affiné nécessiterait des changements significatifs en matière de protocole, éléments de données

Nº.	Principes pour la validation de contact
103.	Pour chaque élément de donnée ayant fait l'objet de validation, l'horodatage de cette validation doit être enregistré et maintenu par le validateur.
104.	L'horodatage du changement le plus récent du statut global de validation pour l'ID complet d'un contact doit aussi être défini par le validateur et publié comme un nouvel élément de donnée du contact dans le RDS.

g. Capacité à détenir des données de contact uniques

Afin de lutter contre l'usurpation d'identité, la diffamation et l'abus, un détenteur de contact peut indiquer que ces données de contact sont uniques et ne doivent pas être utilisées par d'autres revendicateur du détenteur de contact.

a) Les données uniques pourraient inclure plusieurs éléments d'un jeu de contact, notamment l'adresse de courriel et le numéro de téléphone. Il peut être difficile, voire impossible de garantir l'unicité des adresses et des noms.

b) Si un détenteur de contact demande une désignation d'unicité, il doit y avoir un mécanisme fourni aux autres validateurs pour comparer un jeu de données de contact requis avec le détenteur de contact, et s'assurer que des candidats à un nouvel ID de contact (ou des détenteurs de contact existants qui modifient leurs informations) n'empiètent pas sur des données protégées de manière unique.[23]

c) Toutes données désignées comme uniques doivent être validées du point de vue identité pour éviter l'usurpation d'identité et les attaques de type « déni de service » (le contact légitime incapable d'utiliser ses vraies données).

h. Résumé des principaux avantages en matière de qualité des données

L'adoption des systèmes de validation et de gestion des ID de contact en tant que partie intégrante du RDS de nouvelle génération améliorera la qualité des données en rendant plus difficile pour les titulaires de noms de domaine d'insérer de fausses données dans le RDS et réduisant les incidences de fraude et d'usurpation d'identité. Plus particulièrement, les avantages qui résulteraient de l'adoption des principes d'exactitude et de validation de données recommandés par l'EWG comprennent ce qui suit.

---

et interfaces. Ceci n'est donc pas recommandé en ce moment mais pourrait être étudié de manière plus approfondie.

[23] Cette vérification d'unicité peut être effectuée relativement facilement dans le modèle de RDS synchronisé mais peut être plus difficile à effectuer dans le modèle de RDS fédéré.

- Une capacité accrue pour les individus et les organisations de contrôler et de maintenir leurs propres données de contact où qu'elles soient utilisées dans l'écosystème des noms de domaine.
- Rendre plus difficile pour les personnes de mauvaise foi d'obtenir des noms de domaine, puisque tous les contacts doivent être validé à un niveau minimum au moment de la création ou des mises à jour. Les exigences d'accréditation du validateur devraient permettre l'identification et la pénalisation des validateurs laxistes ou escrocs qui ne satisfont pas les normes opérationnelles. En cas d'identification de personnes malveillantes via l'enregistrement d'un seul nom de domaine, les autres noms de domaine détenus par cette même personne peuvent être identifiés et limités via les PBC communs.
- la création de données plus cohérentes à travers les multiples noms de domaine enregistrés par un titulaire de noms de domaine donné. Alors qu'il pourrait y avoir certains coûts initiaux de validation pour un contact donné, le fait de fournir un seul ID de contact portable permet des enregistrements supplémentaires sans frictions et devrait grandement réduire les coûts de maintenance futurs pour un grand nombre de titulaires de noms de domaine.
- La capacité améliorée de détecter des informations de contact non valides au fil du temps et d'appliquer des corrections sur le jeu complet de domaines en utilisant ces informations de contact. Les exigences de vérifications de validation périodiques de la part des validateurs, ou lorsque des mises à jour sont effectuées, devraient mettre en relief les problèmes résultant d'informations de contact obsolètes et appliquer toutes les actualisations à tous les enregistrements de noms de domaine concernés en effectuant un seul changement.
- Des améliorations du coût et de l'efficacité pour l'ensemble de l'écosystème. Alors qu'elle introduit de nouvelles complexités au système d'enregistrements dans son ensemble, la gestion des contacts peut être séparée de la gestion des enregistrements de noms de domaine, permettant l'application de mises à jour à grande échelle aux noms de domaine tout en permettant la localisation de la gestion des données de contact.
- La capacité pour les fournisseurs de services d'actualiser sans entraves les détails des contacts sans avoir à actualiser les enregistrements individuels de noms de domaine pour des noms de domaine dans lesquels ils apparaissent comme contacts basés sur les objectifs. Dans le cas de nombreux fournisseurs, ceci

pourrait permettre des actualisations faciles de milliers voire de millions de noms de domaine.

- Réduire les abus survenant via l'usurpation d'identité dans les données d'enregistrement en fournissant une validation d'identité facultative. Alors que la validation d'identité facultative s'accompagnera probablement d'un certain coût pour le détenteur de contact qui l'obtient, la capacité de réduire les abus via l'usurpation d'identité, systématiquement vécus par les entités de haut niveau, les grands fournisseurs de services ou les individus ciblés, vaudrait bien cette dépense.
- La séparation entre la validation et la gestion des données de contact et la gestion/l'enregistrement du nom de domaine aligne plus étroitement les sujets des données et les données pertinentes, permettant une application plus facile de la loi sur la protection des données puisque les validateurs peuvent être situés dans les juridictions locales des détenteurs de contact, indépendamment du lieu du bureau d'enregistrement ou du registre.
- Les validateurs peuvent fournir des services dans les langues maternelles des détenteurs de contact et des titulaires de noms de domaine, améliorant ainsi la qualité des données et leur exactitude et réduisant les coûts de validation. Ceci pourrait permettre aux bureaux d'enregistrement d'offrir des services dans des langues qu'ils ne pourraient pas facilement seuls soutenir ou valider et ce via un ensemble réparti de validateurs.

VI. Considérations juridiques et contractuelles

Dans son travail, l'EWG a été guidé par certains principes juridiques globaux :

Les données personnelles doivent être : • traitées de manière légale, équitable et transparente en rapport avec le sujet des données, • collectées à des fins spécifiques, explicites et légitimes et traitées par la suite de manière compatible avec ces objectifs, • appropriées, pertinentes et limitées au minimum nécessaire en rapport avec les objectifs pour lesquels elles sont traitées et • exactes et toujours à jour tel que requis pour les objectifs spécifiés.
Le traitement légal, y compris le transfert et la divulgation peut être - sous réserve de la juridiction pertinente - basé sur : • le consentement du sujet des données, • la nécessité d'exécuter un contrat dans lequel le sujet des données est partie contractante et • la nécessité de conformité aux obligations juridiques qui régissent le contrôleur.
Un droit d'accès aux informations et un droit de rectifier les inexactitudes doivent être assurés au sujet des données.

L'EWG recommande que ces principes et d'autres principes pertinents habituellement trouvés dans la législation sur la protection des données devraient être pris en considération lors de la rédaction des politiques finales et des processus de mise en œuvre pour le RDS. En outre, on sait bien que dans certaines juridictions, les droits à la vie privée couvrent les personnes morales et les entités quant à la liberté d'expression et la liberté d'association. L'EWG reconnait ces deux ensembles de droits séparés qui sont protégés séparément et différemment de par le monde.

Ceci étant donné, l'EWG a évalué les options et formulé ensuite des principes du RDS pour la protection de la vie privée et des données et pour l'accès aux représentants de la loi. Ces principes de l'EWG sont présentés dans cette section, soutenus par des principes pour la conformité contractuelle, la responsabilité et l'audit.

a. Principes de protection des données

Aujourd'hui, les pratiques qui prétendent aborder la législation nationale en vigueur en matière de vie privée et de protection du consommateur sont inégales. Certaines lois exigent que lorsque les données sont exportées en dehors de la juridiction de l'individu ou de la personne en charge du traitement des données régis par cette loi, des protections de données similaires ou équivalentes soient appliquées. La directive européenne relative à la protection des données de 1995 ne permet pas le transfert des données en dehors de cette juridiction sauf si la loi locale est évaluée comme « adéquate ». Plusieurs juridictions en dehors de l'UE ont recherché des dispositions contractuelles plus fortes mais dans tous les cas, la plupart des lois exigent que ceux qui détiennent des données personnelles ne les transfèrent ou ne les divulguent pas sans consentement sauf si la protection est garanties. La responsabilité peut être imputée au point de transfert. Pour l'instant, l'ICANN a abordé ce point en permettant une dispense dans le RAA aux bureaux d'enregistrement qui démontrent qu'ils sont sujets à une loi relative à la protection des données qui interdirait le dépôt de données. Ce n'est pas la seule disposition dans l'écosystème de l'ICANN qui représente un risque pour ceux qui cherchent à respecter la loi relative à la protection des données. Il a donc été suggéré que le status quo doit être soigneusement examiné. Étant donné que l'EWG s'est concentré sur la responsabilité dans son travail, l'exigence de responsabilité du point de vue protection des données a été examinée.

Pour l'instant, le fait qu'il soit exigé que l'entité recevant les données personnelles doive garantir une protection des données qui soit appropriée et cohérente avec les protections fournies au sujet des données « chez lui » devrait être satisfaite **au cas par cas**, en fonction de la mesure dans laquelle la juridiction régissant l'entité qui reçoit les données fournit une protection des données légiférée ou une protection similaire appropriée. Ceci signifie que soit l'adéquation est assurée par la loi applicable à l'entité qui reçoit les données soit d'autres garanties sont mises en place permettant que le transfert des données soit légal selon la loi régissant le sujet des données.

Mécanismes de protection des données

Vu la situation actuelle, quatre options progressives pour la protection des données personnelles dans l'écosystème du RDS ont été examinées :

(0) ne rien faire ;

(1) introduire des mécanismes pour faciliter la collecte et le transfert de routine et légalement conforme des données ;

(2) introduire des mécanismes qui visent à harmoniser la confidentialité et la protection des données dans l'écosystème de l'ICANN, pour fournir un « seuil » de base de protection des données qui établisse les bonnes pratiques acceptées de politique relative à la vie privée et

(3) soumettre cette politique comme ensemble de « règles d'entreprise contraignantes ».

Note : Dans cette section, « l'écosystème du RDS » se réfère à tous les acteurs énumérés dans la section VIII(c) relations contractuelles et conformité et la section VIII(d) responsabilité et audit. Ceci inclut l'ICANN (société américaine à but non lucratif), tous les registres et bureaux d'enregistrement de gTLD (chacun fonctionnant comme entreprise indépendante basée dans plusieurs pays) et toutes les nouvelles entités accréditées proposées par l'EWG dans ce document : le fournisseur du RDS, les validateurs, les approbateurs d'identifiants protégés sécurisés, les accréditeurs d'utilisateurs du RDS, la conformité de l'ICANN et autres entités impliquées dans le traitement des données personnelles.

Option (0) : « Ne rien faire »

Ne rien faire résulterait en une très grande complexité à cause du risque continuel de non conformité à la loi relative à la protection des données et de la nécessité d'examiner chaque enregistrement pour déterminer la loi applicable. Ceci créerait des frais généraux coûteux pour certains opérateurs, notamment les registres. Pour les bureaux d'enregistrement ceci pourrait imposer un coût élevé de suivi de l'adéquation de la protection requise par les titulaires de noms de domaine et par les registres. Ceci augmenterait le potentiel d'incertitude légale pour toutes les parties, y compris l'ICANN et les autres parties prenantes dans le système des noms de domaine. La hausse du nombre de gTLD et la variété des emplacements des registres créent de nouveaux défis concernant la législation et la juridiction applicables pour les régimes contractuels de l'ICANN qui ont trait à la vie privée du titulaire de nom de domaine et à la protection du consommateur. Désordre, incertitude et pratiques inégales nécessiteraient plus d'efforts de la part de l'ICANN afin d'assurer la conformité contractuelle et de réduire le risque potentiel. Ces défis existent indépendamment de la question d'un RDS. Avec l'introduction de plus de 1000 gTLD, la question prend de l'ampleur. Et de plus, la protection du sujet des données ne peut pas être garantie de manière cohérente. Un cadre pour une harmonisation qui réduise le risque, minimise la charge et diminue la complexité serait dans l'intérêt de chaque partie prenante.

Option (1) : Introduire des mécanismes pour faciliter la collecte et le transfert de routine et légalement conforme des données ;

La deuxième option envisagée est l'introduction d'un système qui évaluerait la loi sur la vie privée et la protection des données pertinente et présenterait la législation dans une liste pour que les parties prenantes puissent l'appliquer et que les individus soient au courant du lieu de leurs données et de la loi appliquée. Cette liste pourrait être automatiquement appliquée par le RDS par le biais d'un « moteur de règles » tel que défini dans la section suivante. Si un individu vit dans un pays qui a une loi sur la protection des données et que cette loi s'applique en dehors du pays aux données personnelles transférées de la part de l'individu à une autre partie (dans ce cas le bureau d'enregistrement), cette loi pourrait s'appliquer. Si le bureau d'enregistrement est situé dans un pays dont les lois relatives à la protection des données s'appliquent à tous les individus (et non seulement à ses propres citoyens), cette loi s'appliquerait alors certainement. Les données en question ou en rapport avec nos objectifs sont uniquement celles collectées dans le RDS[24]. Codifier les données relatives aux juridictions qui s'appliquent à l'écosystème simplifierait la vie des parties prenantes concernées, assurerait les droits de protection des données (le cas échéant) pour le titulaire du nom de domaine et réduirait le risque de non conformité. Toutefois, dans des juridictions sans loi sur la protection des données s'appliquant au secteur de l'enregistrement de noms de domaine, aux registres ou à l'ICANN et ses mécanismes de conformité, ce scénario offre peu de protection au particulier titulaire de nom de domaine. Ceci pourrait résulter en un système de droits relatifs à la vie privée à plusieurs niveaux, certains particuliers titulaires de nom de domaine n'en ayant aucun et certains ayant pleins droits de l'homme et des motifs d'action sous supervision judiciaire.

Option (2) : Introduire des mécanismes qui viseraient à harmoniser la protection des données dans l'écosystème de l'ICANN, pour fournir un « seuil » de base de protection des données qui privilégie les bonnes pratiques acceptées de politique relative à la vie privée.

Des clauses contractuelles pourraient être rédigées pour rectifier les lacunes dans la protection de la vie privée (reprises dans le volet mise en œuvre) et ces clauses pourraient être basées sur une suite communément acceptée de protections de la vie

[24] Ceci ne faciliterait pas nécessairement les choses pour le bureau d'enregistrement qui contrôle des données beaucoup plus sensibles, telles que des données bancaires, des informations de cartes de crédit, des inscriptions de services clientèle, etc. qui ne sont pas transférées au RDS, bien qu'un « moteur de règles » soit certainement plus utile dans certaines situations, vue la complexité du système gTLD prochain.

privée, qui formerait la base d'une politique de l'ICANN sur la vie privée. Cette politique pourrait être concise, énumérant les clauses pertinentes dans une annexe. Ceci pourrait permettre un transfert illimité de données entre les acteurs de l'écosystème du RDS en offrant un niveau de protection des données assez élevé pour éviter les objections pour des motifs de confidentialité personnelle, de protection des données et de droits des consommateurs.

Les mécanismes visant à faciliter la collecte et le transfert légalement conforme des données dans le système du RDS pourraient prendre différentes formes mais seraient tous basés sur une politique cohérente de protection des données applicable au RDS. L'ICANN imposerait cette politique à toutes les parties prenantes par le biais de dispositions contractuelles, comme elle le fait avec la plupart des autres politiques.

Option (3) : Tirant parti de l'option (2), la politique élaborée pourrait être soumise comme un ensemble de « règles d'entreprise contraignantes », tel que reconnu par l'APEC et l'UE dans la loi relative à la vie privée et à la protection des données.

Cette option simplifierait les transferts de données parmi les 28 états membres dans l'Union européenne, puisqu'elle fournit une définition de protection adéquate des données pour les objectifs des états de l'UE, éliminant la nature ad hoc des décisions sur la protection des données dictées par les flux de données à travers l'écosystème du RDS. Bien que cette option puisse nécessiter plus de temps, elle pourrait réduire le risque de non conformité et assurer une meilleure protection. Elle offirait aussi une supervision indépendante de la politique relative à la vie privée.

Nº.	Résumé des mécanismes de protection de données envisagés
(0)	Ne rien faire.
(1)	Une solution minimum a) identifierait les transferts pour lesquels une protection de vie privée adéquate est assurée par la loi et publierait la liste pertinente et b) introduirait des règles communes dans le contrat pour les acteurs de l'écosystème du RDS dont les transferts ne seraient pas protégés juridiquement de manière appropriée, donnant à la fonction de conformité une seule et simple plateforme pour la maintenance.
(2)	Une politique de confidentialité de l'ICANN pour le RDS pourrait être rédigée, basée sur les bonnes pratiques standard relatives à la protection de la vie privée et des clauses contractuelles standard pourraient être élaborées mettant en vigueur cette politique dans l'écosystème du RDS. Des clauses standard

	pourraient être inclues dans tous les contrats passés entre l'ICANN et tous les acteurs de l'écosystème du RDS engagés dans des transferts de données, assurant un niveau de protection des données assez élevé pour permettre un transfert illimité au sein de cet écosystème.
(3)	L'ICANN étant une société multinationale à but non lucratif, l'écosystème du RDS entier sous son contrôle pourrait être sujet à l'instrument de règles d'entreprise contraignantes (BCR) qui ont prouvé être efficaces permettant au niveau mondial des transferts de données au sein d'une organisation. Dans ce cas, l'écosystème devient le sujet pour la conformité. L'ICANN peut être considérée comme agissant en tant que « contrôleur des données », pour utiliser la terminologie de l'APEC et de l'UE, établissant la politique et les exigences contractuelles.

Évaluation :

Option (0) Ne rien faire. Vue la complexité mondiale croissante du système, et la focalisation sur une exactitude et responsabilité accrues, ceci a été considéré inacceptable.

Option (1) Mécanismes pour faciliter la collecte et le transfert de routine et légalement conforme des données. Cette option serait plus complexe et plus dynamique, les lois changeant dans les différentes juridictions. Elle devrait considérer un flux de données complexe au sein de l'écosystème. Tel que discuté auparavant, un particulier titulaire de nom de domaine peut avoir un bureau d'enregistrement dans une juridiction différente, utiliser un validateur dans une troisième juridiction, maintenir des données dans un registre régi par une quatrième juridiction et dépendre d'un fournisseur de RDS dans une cinquième juridiction.

Option (2) Clauses contractuelles standard qui viseraient à harmoniser la protection des données à travers l'écosystème du RDS. Ce choix pourrait nécessiter une conformité avec la loi en vigueur de la part des parties prenantes, notamment des titulaires de noms de domaine, des bureaux d'enregistrement, des registres et de l'ICANN. Ceci pourrait aussi inclure les nouveaux acteurs du RDS recommandés dans ce rapport : validateurs, fournisseur de RDS, accréditeurs d'utilisateurs du RDS, etc.

En plus de l'obligation de conformité avec les lois locales relatives à la protection des données, cette option, énumérant les éléments communs provenant de la loi relative à la protection des données de l'APEC et de l'UE, contribueraient sensiblement à assurer la conformité. Les clauses pourraient spécifier les conditions de consentement, les droits d'accès, les politiques de rétention et autres éléments (par exemple) en incorporant les

exigences de l'UE sur le traitement légal des données et des éléments appropriés abordés par les règles d'entreprise contraignantes. De telles clauses de contrat standard n'exigeraient pas nécessairement l'autorisation/le suivi par les autorités de protection des données, sauf dans les juridictions où de telles autorisations sont obligatoires.

Option (3) (BCR pour l'écosystème du RDS) En plus de l'obligation de conformité avec les lois locales relatives à la protection des données, cette option pourrait énumérer des éléments communs provenant de loi relative à la protection des données de l'APEC et de l'UE. Comme dans l'option (2), les clauses pourraient spécifier les conditions de consentement, les droits d'accès, les politiques de rétention et autres éléments (par exemple) en incorporant les exigences de l'UE sur le traitement légal des données et des éléments appropriés abordés par les règles d'entreprise contraignantes. De telles clauses de contrat standard n'exigeraient pas nécessairement l'autorisation/le suivi par les autorités de protection des données, sauf dans les juridictions où de telles autorisations sont obligatoires. Toutefois, les BCR devraient être adaptées aux spécifications de l'écosystème du RDS. Les BCR sont sans aucun doute plus applicables aux entreprises ayant une structure de contrôle traditionnelles qu'elles ne le sont à un écosystème connecté de façon lâche tel que géré par l'ICANN. Mais il est certain que les entreprises multinationales mettent en application leurs règles contraignantes relatives à la vie privée par le biais d'exactement le même type de contrat que l'ICANN utilise pour accréditer et contrôler ses parties prenantes.

En conclusion, « ne rien faire » n'est pas une vraie option, spécialement si les recommandations de l'EWG pour l'amélioration de l'exactitude et de la responsabilité sont acceptées. L'option (1) serait bien complexe juridiquement et n'offre pas des droits égaux à tous les titulaires de noms de domaine alors que l'option (3) soulève des soucis quant à l'applicabilité au sein de l'écosystème du RDS (c'est à dire les règles d'entreprise contraignantes sont-elles faisables, seraient-elles acceptées et quelles seraient les implications pour l'ICANN en termes de responsabilité ?).

Par conséquent, l'EWG recommande l'option (2) – élaborer une politique utilisant des clauses contractuelles standard qui sont harmonisées avec les lois sur la protection des données pour mettre en œuvre les exigences de la politique et assurer par le biais de mécanismes d'audit variés que ces protections de vie privée sont imposées par le biais de contrats entre tous les acteurs de l'écosystème du RDS impliqués dans le maniement d'informations personnelles.

Mise en oeuvre de mécanismes de protection des données

Pour tous les scénarios ci-dessus, la question de la mise en œuvre du RDS est opportune - notamment concernant la localisation du fournisseur du RDS.

Si le RDS va détenir des données personnelles, il serait convenable que ces données soient situées dans une juridiction qui fournit des droits de protection de données imposables afin d'éviter les questions relatives à la légitimité des transferts de données et à la responsabilité en cas de violation des données. Cette question est claire si le RDS détient des données qui sont résidentes et situées au même lieu que le responsable de traitement de données. Un cadre de considération similaire devrait s'appliquer même si les données ne sont pas résidentes mais apportées pour traitement (par ex. validation) et envoyées ailleurs par la suite. Trois options de mise en œuvre de protection des données ont été considérées par l'EWG :

Nº.	Résumé des mises en œuvre de protection de données considérées
(0)	« Ne rien faire » s'applique si le niveau de protection des données juridique applicable à l'emplacement du RDS n'est pas pris en considération lorsque le choix géographique est fait. Ce faire pourrait résulter en la localisation du RDS dans une juridiction offrant un bas niveau de protection des données.
(1)	Le RDS pourrait prévoir un cloisonnement juridique. Plus spécifiquement, les éléments de données pourraient être libellés selon la loi applicable au sujet des données (c'est-à-dire le titulaire du nom de domaine) et traités en conséquence. Pour réaliser ce cloisonnement juridique, le RDS pourrait mettre en œuvre un « moteur de règles » qui appliquerait les lois sur la protection des données applicables à chaque transfert spécifique. Plus spécifiquement, le « moteur de règles » se réfère à une caractéristique qui pourrait être mise en œuvre au sein du RDS pour gérer (a) le stockage, la collecte et le traitement des informations du nom de domaine sur la base des juridictions du titulaire du nom de domaine, du contact, du bureau d'enregistrement, du registre et du RDS (représentée par les éléments de données suivants : code pays du titulaire du nom de domaine et du contact, juridictions du bureau d'enregistrement et du registre), et (b) les lois sur la protection des données des juridictions en vigueur, selon la politique future définie par l'ICANN pour le RDS. Ceci est intrinsèquement complexe, tel que décrit ci-dessus, et difficile à imposer si le RDS est dans une juridiction sans loi sur la protection des données qui fournit un accès aux tribunaux.

Nº.	Résumé des mises en œuvre de protection de données considérées
(2)	La localisation du RDS est choisie selon le critère de transfert des données le plus facile et le moins compliqué. Ce faire impliquerait choisir un ou des lieux pour le stockage des données du RDS où la loi nationale en vigueur sur la protection des données offre un niveau de protection élevé.

Évaluation :

L'**option (0) « ne rien faire »** maintient le status quo et augmente la complexité de plusieurs transferts de données en :

- restaurant un processus qui rend difficile, et presque impossible en pratique, de respecter les cadres juridiques ;
- infligeant des charges administratives et juridiques aux bureaux d'enregistrement ainsi qu'à d'autres acteurs dans l'écosystème, y compris la conformité de l'ICANN et
- étant loin d'être transparent concernant la loi locale sur la protection des données et la conformité en matière de vie privée et n'étant pas extensible.

L'**option (1) cloisonnement juridique via un « moteur de règles »** est innovatrice, mais sa faisabilité reste à tester du point de vue technique. Juridiquement parlant, il y a un nombre de questions ouvertes, notamment concernant la définition, l'acceptation juridique et la mise en œuvre d'un tel système.

L'**option (2) localisation des données dans une ou des juridictions sélectionnées** pourrait être une solution simple et élégante pour offrir un niveau de protection très élevé à tous les mouvements de données. Toutefois, cette option ne permet en soi d'appliquer les lois locales sur la protection de données régissant chaque sujet.

L'option (0) n'étant pas faisable et les options (1) et (2) n'étant pas mutuellement exclusives*, l'EWG recommande que les deux options (1) et (2) soient prises en considération pour l'instant comme moyen de mettre en œuvre un niveau de protection de données élevé à assurer par le biais de politique et de clauses contractuelles standard.*

Après avoir considéré toutes ces options relatives aux politiques de protection de données, aux mécanismes et à la mise en œuvre, l'EWG a convenu des principes suivants :

Nº.	Principes de protection des données
105.	Des mécanismes doivent être adoptés pour faciliter la collecte de données de routine conforme d'un point de vue juridique et le transfert entre les acteurs au sein de l'écosystème RDS.
106.	Des clauses de contrat standard qui soient harmonisées avec les lois sur la vie privée et la protection des données devraient être codifiées dans une politique et imposées par le biais de contrats entre tous les acteurs de l'écosystème du RDS impliqués dans le maniement d'informations personnelles.
107.	Un système informatique pour appliquer les lois sur la protection des données (c'est-à-dire un « moteur de règles ») et la localisation du stockage des données du RDS doivent être considérés comme deux moyens de mise en œuvre du niveau de protection des données élevé requis. Ceci doit être assuré via des clauses contractuelles standard, qui dérivent d'une politique de confidentialité logique pour l'écosystème du RDS.

b. Principes pour l'accès aux données de la part des représentants de la loi

A la différence du cas de protection de données, la protection juridique du sujet des données dans les cas d'accès des représentants de la loi ne peut pas être « exportée ». Pour l'accès des représentants de la loi, trois options sont envisagées.

Nº.	Résumé des options d'accès des représentants de la loi considérées
(0)	« Ne rien faire ». L'accès des représentants de la loi suivrait les règles existantes dans la mesure où les représentants de la loi nationaux auraient accès aux données du RDS entreposées dans chaque référentiel de données au niveau national respectif. Au portail centralisé du RDS, l'accès serait accordé selon la législation nationale du pays d'hébergement du portail du RDS.
(1)	Au niveau du portail central du RDS, où les données ne sont pas publiquement disponibles et où des procédures juridiques spécifiques ne sont pas requises des représentants de la loi selon la législation nationale en vigueur, les conditions d'accès pourraient être spécifiées pour le système du RDS et mises en œuvre de l'une des deux façons : a) Europol et Interpol pourraient passer un accord contractuel avec le RDS pour mettre en œuvre et exécuter un tel système, servant d'intermédiaire actif en temps réel pour tout accès de représentants de la loi et étant responsable de la protection et de l'utilisation appropriées des données.

Nº.	Résumé des options d'accès des représentants de la loi considérées
	b) Europol et Interpol pourraient passer un accord contractuel avec le RDS pour servir d'accréditeurs d'utilisateurs pour la communauté de représentants de la loi, examinant les candidats pour émettre des identifiants RDS qui sont alors utilisés par les agences individuelles pour accéder à des données sécurisées du RDS et être responsables de la protection et de l'utilisation appropriées des données.
(2)	De plus, au niveau central, des mécanismes pourraient être établis qui permettraient l'accès au portail central du RDS de la part des représentants de la loi, même lorsque des exigences spécifiques existent dans les relations bilatérales traditionnelles qui seraient inclues dans les traités d'assistance juridique mutuels (MLAT). Un cloisonnement des données quant à la législation applicable pourrait soutenir l'établissement d'un tel mécanisme.

Évaluation :

Il est clair que l'**option (0) (« ne rien faire »)** n'offre pas une valeur d'accès ajoutée aux représentants de la loi.

L'**option (2) (MLAT au niveau du portail d'accès des utilisateurs du RDS)** il n'est pas prévu que les éléments de données sécurisés recommandée rendus accessibles par le biais du RDS nécessiteraient une autorisation judiciaire supplémentaire pour l'accès des représentants de la loi. Ainsi, il n'est pas nécessaire de considérer l'option (2) de manière plus approfondie.

L'**option (1) (l'approche de portail d'accès des utilisateurs accrédités du RDS)** facilite l'accès aux représentants de la loi. Bien que les deux variantes (1a) et (1b) tireraient parti des structures existantes, la variante (1a) (accès accrédité avec cloisonnement via intermédiaire en temps réel) tirerait également parti des mécanismes existants de coopération des représentants de la loi et éviterait la création d'une couche supplémentaire de complexité. Toutefois, la capacité de détecter et de remédier à des abus individuels potentiels resterait à assurer.

La variante (1a) est examinée dans la section IV(c), accréditation d'utilisateur du RDS, scénario #3, qui décrit en détail comment des accréditeurs potentiels comme Interpol pourraient être des intermédiaires pour les demandes d'accès au RDS autorisé des représentants de la loi tout en décourageant les abus potentiels. Se référer aux principes d'accréditation d'utilisateurs du RDS pour les recommandations pertinentes.

De plus, pour l'option (1), il faut s'assurer que le cadre juridique pour les représentants de la loi nationaux dans la ou les juridictions où les données du RDS sont entreposées ne prévaut pas sur le cadre établi pour le RDS. La géographie de la localisation du RDS est ainsi d'une importance cruciale.

Nº.	Principes d'accès des représentants de la loi
108.	Le RDS doit entreposer des données dans une ou des juridictions où les représentants de la loi sont mondialement crédibles, indépendamment du modèle de mise en œuvre.

c. Principes de conformité et de relations contractuelles

L'EWG recommande l'ensemble suivant de principes concernant les relations contractuelles entre les parties au sein de l'écosystème du RDS :

Nº.	Principes de relations contractuelles
109.	Un fournisseur tiers qui est une organisation non gouvernementale avec un champ d'action mondial devrait gérer le RDS.
110.	L'ICANN doit conclure des contrats appropriés avec ce fournisseur tiers du RDS pour rendre possible la conformité, l'audit et la disponibilité.
111.	L'ICANN doit conclure des contrats appropriés avec des validateurs, fournisseurs de services d'anonymisation/d'intermédiation, approbateurs d'identifiants sécurisés et autres qui pourraient interagir avec le RDS (voir section III(c) principe #1).
112.	L'ICANN doit modifier les accords existants (RAA, accords de registre) pour qu'ils s'adaptent au RDS et éliminer ainsi les vieilles exigences.
113.	Le RDS doit s'appliquer à tous les registres gTLD, autant aux existants qu'aux nouveaux. Aucun droit historique ou exemption particulière ne devraient être accordés.

d. Principes de responsabilité et d'audit

L'EWG recommande que les acteurs de l'écosystème du RDS soient tenus responsables des actions relatives aux informations d'enregistrement, comme suit :

Nº.	Principes de responsabilité et d'audit
114.	Toutes les entités au sein de l'écosystème du RDS doivent être tenues responsables de l'une ou plus des exigences indiquées dans le tableau 6 :

Nº.	Principes de responsabilité et d'audit
	a) fournir des informations d'enregistrement exactes et fiables b) utiliser les informations uniquement pour les objectifs désignés c) sécuriser les informations collectées, entreposées ou transmises d) valider ou authentifier les informations lorsqu'elles sont collectées e) actualiser les informations précédemment fournies de manière opportune f) imposer les politiques de confidentialité et les conditions d'utilisation (ToU) du RDS g) détecter les abus d'informations d'enregistrement h) traiter et suivre les plaintes i) se conformer aux politiques ToU et ToS établies j) établir des mécanismes pour décourager la récolte de données de la part de tiers et la création de comptes frauduleuse en vrac. k) établir un processus permanent d'audit et de correction Les parties prenantes suivantes[25] ont des rôles de responsabilité dans l'écosystème du RDS : a) Utilisateurs du RDS en quête de données (USD) - énumérés dans la section III b) Titulaires de noms de domaine c) Bureaux d'enregistrement[26] d) Registres[27] e) Fournisseur de services d'annuaire d'enregistrement f) ICANN g) Fournisseurs de services d'anonymisation ou d'intermédiation h) Approbateur d'identifiants sécurisés et protégés i) Validateurs j) Accréditeurs d'utilisateurs du RDS k) Contacts basés sur les objectifs l) Fournisseurs de dépôt fiduciaire
115.	Le RDS doit établir des procédures pour le maniement de plaintes relatives à la non disponibilité de données, l'utilisation inappropriée de données, l'accès non autorisé à des données, les infractions de politique de confidentialité et les saisies de données inexactes ; par exemple : Des éléments de données de

[25] Ces rôles et responsabilités s'étendent aux agents des parties prenantes et aux préposés (par ex. les revendeurs)

[26] Tel que défini par http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.htm

[27] Tel que défini par http://newgtlds.icann.org/en/applicants/agb/agreement-approved-09jan14-en.pdf

Nº.	Principes de responsabilité et d'audit
	contact en cas d'abus et un portail pour recevoir les plaintes des USD et des titulaires de noms de domaine.
116.	Le RDS doit établir des recours progressifs concernant les données inexactes ; par exemple : Avertissement par courriel, marquage des inscriptions visible pour l'utilisateur/navigateur, action de la part du département de conformité de l'ICANN, et autres motivations pour encourager l'exactitude. (Voir la section V améliorer la qualité des données pour les exigences d'exactitude).
117.	Le RDS doit établir des recours progressifs concernant l'accès non autorisé à des données ; par exemple : Avertissement par courriel, limitation de débit, blocage temporaire, suspension d'accréditation, résiliation et autres éléments dissuasifs. (Voir la section IV améliorer la responsabilité pour les exigences d'accès sécurisé).
118.	Le RDS doit établir des recours progressifs concernant l'usage non approprié de données ; par exemple : Avertissement par courriel, limitation de débit, blocage temporaire, suspension d'accréditation, résiliation et autres éléments dissuasifs. (Voir la section III utilisateurs et objectifs pour les objectifs admissibles).
119.	Le RDS doit établir des mécanismes d'audit afin de détecter les abus d'identifiants d'accès au RDS et les violations de ToU ; par exemple : des mécanismes pour détecter les schémas de comportement insolites. (Voir la section IV améliorer la responsabilité pour les exigences d'accès sécurisé).
120.	Le RDS doit établir des mécanismes d'audit afin de détecter les abus de données d'enregistrement pour des usages autres que les objectifs énoncés ; par exemple : des mécanismes pour détecter les schémas de comportement insolites. (Voir la section III utilisateurs et objectifs).
121.	Le RDS doit établir des mécanismes d'audit afin de détecter les abus par des validateurs ; par exemple : formation des validateurs, échantillonnage aléatoire périodique de données à vérifier pour assurer une validation correcte. (Voir la section V améliorer la qualité des données)
122.	Le RDS doit établir des mécanismes d'audit afin de détecter les abus par des accréditeurs d'utilisateurs du RDS ; par exemple : établir des mécanismes pour détecter les schémas de comportement insolites. (Voir la section IV améliorer la responsabilité pour la définition des abus).

Nº.	Principes de responsabilité et d'audit
123.	Le RDS doit établir des mécanismes d'audit afin de détecter les abus par des fournisseurs d'anonymisation/d'intermédiation et des approbateurs d'identifiants sécurisés ; par exemple : établir des mécanismes pour détecter les schémas de comportement insolites. (Voir la section IV améliorer la responsabilité pour la définition des abus).
124.	Les USD du RDS doivent être d'accord avec l'audit de l'accès aux données, l'utilisation et la fourniture d'informations exactes relatives à l'identité et à l'objectif dans les conditions d'utilisation (ToU).
125.	Le RDS doit établir un processus pour corriger, suspendre ou résilier des validateurs si les données ne sont pas adéquatement validées, entreposées et sécurisées. (Voir la section V améliorer la qualité des données pour les exigences relatives aux validateurs).
126.	Le RDS doit établir un processus pour corriger, suspendre ou résilier des approbateurs d'identifiants sécurisés si le contrôle n'est pas correct ou adéquat. (Voir la section VII améliorer la vie privée du titulaire du nom de domaine pour les exigences).
127.	Le RDS doit établir un processus pour corriger, suspendre ou résilier des accréditeurs d'utilisateurs du RDS si les USD ne sont pas adéquatement accrédités, entreposés et sécurisés. (Voir la section IV améliorer la responsabilité pour les exigences d'accréditeurs d'utilisateurs du RDS).
128.	L'ICANN doit établir des politiques de ToS pour s'assurer que les registres, les bureaux d'enregistrement et les validateurs fournissent des données exactes, actualisées et opportunes au RDS. (Voir la section VI considérations juridiques et contractuelles pour les exigences du RDS et du registre, devant être reflétées dans le RIA et le RAA).
129.	Le RDS doit établir un processus d'audit pour les registres, les bureaux d'enregistrement et les validateurs et un processus de signalement à l'ICANN si le registre/le bureau d'enregistrement/le validateur ne fournit pas des données exactes, actualisées et opportunes. (Voir la section VI considérations juridiques et contractuelles pour les exigences du RDS et du registre, devant être reflétées dans le RIA et le RAA).
130.	Le RDS doit établir des mécanismes d'audit pour assurer la qualité et l'intégrité continues des données collectées par le RDS et entreposées auprès du fournisseur de dépôt fiduciaire. (Voir la section VIII Dépôt fiduciaire et

Nº.	Principes de responsabilité et d'audit
	inscription de données)
131.	L'ICANN doit établir des mécanismes d'audit afin de détecter des infractions des ToC de la part du fournisseur de RDS. Par exemple : permet l'usage non autorisé des données, ne répond pas aux plaintes concernant les abus de données, les abus d'identifiants ou de validation. (Voir la section VI considérations juridiques et contractuelles)
132.	L'ICANN doit établir un processus pour corriger, suspendre ou résilier le fournisseur de RDS s'il n'honore pas ses responsabilités contractuelles. Par exemple : disponibilité, fiabilité, vie privée, droits d'accès et exigences de performance. (Voir la section VI considérations juridiques et contractuelles)
133.	L'ICANN doit définir et mesurer les améliorations annuelles accomplies pour réaliser les buts principaux du RDS : (I) qualité des données améliorée, (ii) responsabilité améliorée, (iii) vie privée améliorée. Le RDS doit démontrer un progrès durable dans les trois domaines à des rythmes similaires, avec un processus pour identifier et remédier à des problèmes imprévus qui font qu'un domaine s'améliore plus lentement que les autres.

Le tableau suivant résume les entités de l'écosystème du RDS et les types d'exigences de responsabilité et d'audit qui devraient s'appliquer à eux, faisant suite au principe 114.

Exigences applicables	Utilisateur du RDS en quête de données	Titulaire de nom de domaine	Bureau d'enregistrement	Registre	Fournisseur RDS	ICANN	Fournisseur d'accès à Internet / système d'exploitation	Approbateur identifiant sécurisé	Validateur	Accréditeur d'utilisateurs du RDS	Contact basé sur objectif	Fournisseur de dépôt fiduciaire
Fournit des données exactes/fiables		✔	✔	✔	✔		✔	✔	✔		✔	✔
Utilise pour un objectif désigné	✔		✔	✔	✔	✔	✔	✔	✔			✔
Sécurise les informations			✔	✔	✔	✔	✔	✔	✔			✔
Valide/authentifie					✔				✔	✔		
Actualise de manière opportune		✔	✔	✔			✔	✔	✔		✔	
Impose des politiques de confidentialité			✔	✔	✔	✔	✔	✔	✔			✔
Détecte les abus					✔	✔				✔		
Traite les plaintes			✔	✔	✔	✔	✔	✔	✔	✔		
Décourage la récolte de la part de tiers				✔	✔				✔			
Contrôle et remédie					✔	✔				✔		

Tableau 6 : Exigences de conformité pour les entités de l'écosystème du RDS

VII. Améliorer la vie privée du titulaire du nom de domaine

L'élément central du mandat de l'EWG est la question de la conception d'un système qui augmente l'exactitude des données collectées tout en offrant également les protections pour les titulaires de noms de domaine cherchant à garder et maintenir leur vie privée. L'EWG reconnait que les informations personnelles sont protégées par les lois relatives à la protection de la vie privée, et que même lorsqu'il n'y a pas de loi, il y a des raisons légitimes pour les individus de chercher une plus grande protection de leurs informations personnelles. De plus, les entreprises et les organisations peuvent chercher une protection de leurs informations à des fins légitimes, comme lorsqu'elles sont en train de préparer le lancement d'une nouvelle ligne de produits, ou, dans les cas de petites entreprises, lorsque les coordonnées divulguent des données personnelles.

Par conséquent, l'EWG recommande les principes suivants de base :

Nº.	Principes relatifs à la vie privée
134.	En plus du respect de la vie privée garanti par la conformité aux lois de protection des données, l'écosystème du RDS doit desservir des besoins concernant la vie privée en incluant : • Un service d'anonymisation/d'intermédiation accrédité pour la protection générale des données personnelles et le respect de la loi locale sur la vie privée et • Un service de protection d'accès aux informations par identifiants sécurisés accrédité pour les personnes à risque et dans le cas où les droits à la liberté de parole ne seraient pas respectés ou les orateurs persécutés.
135.	Il doit y avoir un système d'accréditation des fournisseurs d'anonymisation/d'intermédiation, ainsi que des règles pour la fourniture et l'utilisation des services accrédités d'anonymisation/d'intermédiation.
136.	En dehors des noms de domaine enregistrés par le biais de services accrédités d'anonymisation/d'intermédiation, tous les titulaires de nom de domaine doivent assumer la responsabilité des noms de domaine qu'ils enregistrent.
137.	L'ICANN doit envisager l'élaboration d'une politique unique, harmonisée relative à la vie privée qui régisse les activités du RDS de manière complète, tel que décrit ci-dessous.

En plus des lois de protection des données, d'autres lois et constitutions nationales sur la vie privée protègent les droits de milliers de millions d'internautes qui s'expriment en ligne et expriment leurs points de vue sans que ces opinions ne soient facilement et immédiatement attribuables à leurs noms et adresses. Ces lois sur la vie privée comprennent la déclaration des droits de l'homme des Nations Unies (Article 19)[28] qui protège les droits de liberté d'expression et de parole et préserve la capacité et même l'obligation des groupes, organisations, individus et entreprises (tels que les médias et la presse) de réviser et critiquer les pratiques des dirigeants, l'exercice du pouvoir et la direction d'un pays, d'une culture ou d'une société.

Les lois relatives à la vie privée qui protègent la liberté de parole et d'expression reconnaissent souvent le besoin d'exercer ces droits selon des règles qui dissocient les noms et adresses des organisations et groupes du discours qu'ils émettent et qui peut critiquer un gouvernement, une société, une communauté ou un quartier. Elles peuvent encourager le marché des idées, et placent les besoins de communication des sociétés ouvertes au-delà de l'autorité pouvant persécuter les orateurs ou de la possibilité de juger au préalable un message simplement parce que quelqu'un n'apprécie pas son partisan.

Les lois relatives à la vie privée et les droits constitutionnels peuvent aussi protéger la liberté d'association, de religion, d'ethnicité, de moralité et de communauté. Collectivement, elles peuvent exclure le besoin pour les individus ou les organisations de déclarer leurs noms ou mêmes leurs adresses lorsqu'ils exprimes des opinions impopulaires ou minoritaires - de sorte qu'ils ne puissent pas être immédiatement repérés et décriés, ou pire. Dans cette décennie d'agitation politique populaire et d'antagonisme à l'égard de toutes opinions opposées, les lois sur la vie privée protègent les voix minoritaires et préservent la capacité des orateurs en ligne d'exhorter au changement et à la réforme.

Tout au long du présent rapport, lorsque nous parlons de vie privée et de protection des informations personnelles, nous entendons reconnaitre ces deux ensembles de droits séparés, souvent protégés en vertu de législations différentes et de manières différentes de par la planète.

a. Principes relatifs aux services accrédités d'anonymisation et d'intermédiation

Actuellement, il existe des services offerts pour dissimuler l'identité et/ou l'adresse des entités utilisant les noms de domaine. Ceux-ci se sont développés à cause de la nature ouverte du WHOIS. Il existe plusieurs variantes mais l'accord d'accréditation de bureaux d'enregistrement de 2013 définit deux de ces services :

- Un « service d'anonymisation » est un service par lequel un nom enregistré est enregistré au nom de son usufruitier comme titulaire du nom, mais pour lequel des informations de contact alternatives fiables sont fournies par le fournisseur de P/P pour l'affichage de l'information de contact du titulaire du nom enregistré dans le service de données d'enregistrement (WHOIS) ou ses équivalents.
- Un « service d'intermédiation » est un service par lequel un titulaire d'un nom enregistré enregistre l'utilisation d'un nom enregistré au nom d'un client de P/P afin de fournir l'utilisation du nom de domaine au client de P / P, et les informations de contact du titulaire du nom enregistré sont affichées dans le service de données d'enregistrement (WHOIS) ou dans des services équivalents au lieu des informations de contact du client P/P.

Dans ces définitions « fournisseur P/P » ou « fournisseur de services » est le fournisseur de services d'anonymisation/d'intermédiation, y compris le bureau d'enregistrement et ses affiliés, le cas échéant. Le « client P/P » désigne (indépendamment de la terminologie utilisée par le fournisseur P/P), l'exploitant, le client, l'usufruitier, le bénéficiaire ou autre destinataire des services d'anonymisation et d'intermédiation.

Les services d'anonymisation ou d'intermédiation actuels ne sont pas normalisés ; les fournisseurs n'ont pas de relations contractuelles avec l'ICANN, bien que le RAA 2013 introduise le concept d'accréditation par l'ICANN et une ligne de base d'obligations, tel que reflété dans une spécification provisoire. Toutefois, certains fournisseurs sont aussi des bureaux d'enregistrement. Tous les bureaux d'enregistrement sont sujets au RAA, qui stipule ce qui suit concernant les noms de domaine enregistrés par intermédiation :[29]

> 3.7.7.3 Tout titulaire d'un nom enregistré ayant l'intention d'accorder une licence pour l'utilisation d'un nom de domaine à une tierce partie restera néanmoins le titulaire du nom enregistré dans l'archive et il devra fournir toutes ses informations de contact et des renseignements à jour et précis sur les contacts technique et administratif afin de faciliter la résolution opportune de

[29] Le nouveau RAA 2013 a été approuvé par le Conseil d'administration de l'ICANN le 27 juin 2013 ; la section 3.7.7.3 (ici citée) est très peu différente du texte du RAA 2009, sauf concernant l'ajout de la période de 7 jours.

tout problème qui pourrait survenir[30] en rapport avec le nom enregistré. Le titulaire du nom enregistré qui accorde une licence pour l'utilisation d'un nom enregistré conformément à la présente disposition acceptera d'assumer la responsabilité pour tout préjudice causé par l'utilisation illégale du nom enregistré, sauf s'il divulgue l'information de contact actuelle du détenteur de la licence à une tierce partie qui lui apporte la preuve du préjudice passible de poursuites dans les sept (7) jours.

Le WHOIS pour un domaine enregistré aujourd'hui par service d'intermédiation (proxy) apparait plus ou moins comme ceci :

```
  Nom de domaine : EXAMPLE-DOMAIN.COM
      Créé le : 31/10/2011
      Expire le : 31/10/2013
      Dernière mise à jour : 19/09/2012

   Titulaire du nom de domaine :
   Domaines par Proxy, LLC                    ← Nom du titulaire = Proxy
   DomainsByProxy.com                         ← Org titulaire = Proxy
   14747 N Northsight Blvd Suite 111, PMB 309  ← Adresse titulaire = adresse
Proxy
   Scottsdale, Arizona 85260
   États-Unis

   Contact administratif : (nom pour le contact technique)
      Privé, Enregistrement
      example-domain.com @domainsbyproxy.com          ← Email = domain@proxy
      Domaines par Proxy, LLC                         ← Nom = Proxy
      DomainsByProxy.com                        ← Org = Proxy
      14747 N Northsight Blvd Suite 111, PMB 309      ← Adresse = adresse Proxy
      Scottsdale, Arizona 85260
      États-Unis
      (480) 624-2599      Fax -- (480) 624-2598       ← Tel/Fax = Proxy
```

Le WHOIS pour un nom de domaine enregistré aujourd'hui par le biais d'un service d'anonymisation apparait de manière similaire, sauf que le nom du titulaire du nom de domaine (et souvent les noms des contacts administratif et technique) identifient directement le service d'anonymisation et non pas le fournisseur du service proxy.

Il n'existe pas de procédures standard utilisées aujourd'hui par tous les fournisseurs de services d'anonymisation et d'intermédiation. Toutefois, il existe plusieurs besoins communs, souvent soutenus dans une certaine mesure :

- relayer la communication au client service d'anonymisation ou de proxy - souvent réalisé par transmission automatique de courriel envoyé à l'adresse

[30] Note : L'EWG suggère que l'ICANN examine si « tout problème » ne serait pas trop général.

de courriel du contact administratif/technique. Le relais est fourni par de nombreux fournisseurs mais pas par tous.

- La divulgation de l'identité du détenteur de licence et des coordonnées de contact direct d'un client de proxy en réponse à une plainte concernant le nom de domaine. Les procédures, la documentation, la réactivité et les actions prises varient et dépendent souvent des relations établies entre les requérants et les fournisseurs.
- Divulguer l'identité du détenteur de licence, rendant les détails relatifs au nom et aux contacts du client du service proxy publiquement disponibles dans le WHOIS.
- Lorsque les requérants ne peuvent pas contacter un client du service proxy ou obtenir une solution de la part du fournisseur du service proxy, ils s'adressent souvent au bureau d'enregistrement (affilié ou non affilié au fournisseur du service proxy).

Les lacunes dans les services actuels d'anonymisation et d'intermédiation sont bien documentées.[31] Afin d'aborder besoins des titulaires de noms de domaine et des parties prenantes en matière de services d'anonymisation et d'intermédiation plus uniformes et fiables qui permettent une plus grande responsabilité, l'EWG recommande les principes suivants :

Nº.	Principes relatifs aux services accrédités d'anonymisation et d'intermédiation
	Généralités
138.	L'ICANN doit accréditer des fournisseurs de services d'anonymisation et d'intermédiation (P/P)[32].
139.	Comme minimum, le programme d'accréditation doit perpétuer les engagements relatifs aux P/P selon la spécification du RAA 2013.
	Principes relatifs aux services d'anonymisation accrédités

[31] Voir **l'annexe B** pour les études et les rapports qui documentent les lacunes concernant le WHOIS et les services d'anonymisation/d'intermédiation.

[32] La GNSO a établi un groupe de travail pour l'élaboration de politiques relatives à l'accréditation de services d'anonymisation/d'intermédiation. L'EWG recommande que le RDS utilise les fondements établis par ce groupe de travail en les modifiant de sorte à refléter les méthodes d'accès au RDS et ses éléments de données - et surtout les contacts basés sur les objectifs publiés pour les P/P.

Nº.	Principes relatifs aux services accrédités d'anonymisation et d'intermédiation
140.	Les entités et les personnes physiques peuvent enregistrer des noms de domaine via des services d'anonymisation accrédités qui ne divulguent pas les coordonnées de contact du titulaire de nom de domaine sauf dans des circonstances définies (par ex. violation des conditions de service, assignation).
141.	L'ICANN doit exiger que des conditions spécifiques soient inclues dans les conditions de service. Les conditions de service doivent exiger que le fournisseur de service s'efforce à fournir une notification en cas de retraits rapides.
142.	Les services d'anonymisation accrédités doivent fournir au bureau d'enregistrement (utilisant un PBC créé via un validateur) des coordonnées de contact exactes et fiables pour tous les contacts basés sur objectifs obligatoires, afin de joindre le fournisseur de service d'anonymisation et les entités autorisées à résoudre les questions techniques, administratives et autres pour le compte du titulaire du nom de domaine.
143.	Les services d'anonymisation accrédités doivent être obligés de relayer les courriels reçus par l'adresse email de transmission du titulaire du nom de domaine au titulaire du nom de domaine.
	Principes relatifs aux services d'intermédiation accrédités
144.	Les entités et les personnes physiques peuvent enregistrer des noms de domaine via des services d'intermédiation accrédités qui enregistrent les noms de domaine pour le compte de leur client.
145.	Les fournisseurs de services d'intermédiation accrédités doivent fournir au bureau d'enregistrement (utilisant un PBC créé via un validateur) leurs propres coordonnées de titulaire et de contact, y compris une adresse email unique pour la transmission et le contact de l'entité autorisée à enregistrer le nom de domaine pour le compte du client du service d'intermédiation.
146.	En tant que détenteurs du nom enregistré, les fournisseurs de services d'intermédiation accrédités doivent assumer toutes les responsabilités habituelles du titulaire pour ce nom de domaine, y compris la fourniture de données de contacts basés sur objectifs obligatoires et d'autres données d'enregistrement exactes et fiables.
147.	Les services d'intermédiation accrédités doivent fournir au bureau d'enregistrement (utilisant un PBC créé via un validateur) des coordonnées de contact exactes et fiables pour tous les contacts basés sur objectifs obligatoires, afin de joindre le fournisseur de service d'intermédiation et les entités autorisées à résoudre les questions techniques, administratives et

Nº.	Principes relatifs aux services accrédités d'anonymisation et d'intermédiation
	autres pour le compte du client du fournisseur de services d'intermédiation.
148.	Les services d'intermédiation accrédités doivent être obligés de relayer les courriels reçus par l'adresse email de transmission du titulaire du nom de domaine tel que décrit à l'annexe H.
149.	Les services d'intermédiation accrédités doivent être obligés de divulguer les requêtes de manière opportune tel qu'indiqué dans les procédures de transfert décrites à l'annexe H.

b. Principes relatifs aux identifiants sécurisés et protégés

Il a été reconnu que certains particuliers et groupes qui souhaitent maintenir leur anonymat sur Internet, ou au moins éviter que leurs adresses et informations personnelles ne deviennent disponibles à ceux susceptibles de représenter une menace pour eux, ont un besoin légitime de protection de vie privée renforcée. Ces parties peuvent exercer leurs droits conformément à la loi relative à la vie privée lorsqu'elle existe ou utiliser des services d'intermédiation pour l'enregistrement. Mais malheureusement, ces mécanismes peuvent ne pas être assez sécurisés pour ceux qui sont réellement menacés. Si les coordonnées du titulaire du nom de domaine ne sont pas disponibles sur Internet, les poursuivants de ces particuliers ou groupes vont cibler les validateurs, les bureaux d'enregistrement ou les registres avec leurs demandes d'informations, souvent utilisant des techniques d'ingénierie sociale que ces parties sont mal équipées pour détecter.

Le but d'offrir des identifiants protégés sécurisés est de fournir un enregistrement anonyme sûr pour les particuliers ou les groupes menacés. Ceci peut inclure ceux qui souhaitent exercer la liberté d'expression (généralement considérée comme protégée) ou les locuteurs l'identification desquels pourrait constituer une menace pour leur vie ou celle de leur famille.

Voici cinq exemples différents :

1. Minorités religieuses

Dans de nombreuses juridictions il existe des minorités religieuses qui sont menacées par des groupes appartenant à la population ou par des éléments provenant de leurs propres rangs. Ils peuvent souhaiter avoir un site Web pour fournir des informations à leurs membres, tout en maintenant le secret concernant le lieu et leur façon de fonctionner. Par exemple, une synagogue à

Rome ne révèle pas son adresse à cause des alertes fréquentes à la bombe, mais souhaite publier les heures d'office pour les membres qui connaissent l'adresse.

2. Violence conjugale

De nombreuses juridictions offrent une certaine forme de changement d'identité à des personnes qui ont été victimes de violence conjugale ou qui fuient leurs agresseurs. Ceci s'applique aussi à ceux qui fuient certaines communautés religieuses et certains cultes et à ceux qui bénéficient de programmes de protection des témoins. Les refuges pour les femmes victimes de violences conjugales peuvent avoir besoin de faire de la publicité concernant leurs services sut Internet et d'y publier des points de contact sûrs et des instructions pour les victimes réelles afin qu'elles puissent se rendre aux refuges, etc. Des individus et des familles qui ont changé d'identité peuvent souhaiter avoir des sites Web sans jamais divulguer leurs vraies adresses et identités. Il faudrait noter qu'il y a plusieurs individus qui travaillent pour des gouvernements et opèrent sous une autre identité pour diverses raisons, habituellement liées à la sécurité nationale et à l'application de la loi. Ces individus ont aussi besoin d'une protection renforcée sur le terrain et dans leur vie privée.

3. Discours politique

Dans plusieurs pays du monde, un parti de l'opposition ou des candidats perdants peuvent s'enfuir après des élections. Ils peuvent aussi souhaiter avoir un site Web pour fournir des détails sur les évènements dans leur pays d'origine ou la persécution dont ils font l'objet. Le gouvernement au pouvoir peut poursuivre leur site Web, alléguant une trahison ou d'autres crimes, après la publication sur le site Web de la documentation des abus de ce gouvernement. Il s'agit de situations délicates, les droits de liberté de parole variant énormément d'état en état et protégeant rarement contre les allégations de trahison. Le droit d'enregistrer un nom de domaine est tout ce dont l'ICANN et ses bureaux d'enregistrement accrédités ont besoin de se préoccuper.

4. Groupes ethniques ou autres groupes sociaux

Les groupes ethniques font souvent l'objet de harcèlement et de discrimination et peuvent souhaiter avoir des sites Web où ils fournissent des informations cruciales à leurs membres. Par exemple, ils peuvent souhaiter avoir un site Web où les membres puissent publier des incidents de harcèlement sans avoir peur d'identification ou de représailles. D'autres groupes, tels que les communautés de lesbiennes, gays et transsexuels peuvent souhaiter avoir un site Web

ordinaire fournissant des informations à leur communauté mais craignent l'identification des membres compte tenu des lois restrictives dans leur pays ou des représailles de la part de justiciers ou de groupes motivés par la haine. Il existe même des cas de représailles contre des opérateurs de sites qui fournissent des informations relatives à la santé et à l'alimentation à des femmes, des informations relatives aux droits de reproduction, etc.

5. Journalistes opérant dans des territoires hostiles

Les journalistes publiant des articles dans des territoires hostiles peuvent avoir besoin ou souhaiter avoir un site Web tout en maintenant l'anonymat et la sécurité concernant leurs identités et leurs adresses, y compris celles de leurs collaborateurs, traducteurs, etc.

Examen de technologies relatives aux identifiants sécurisés

Il existe divers identifiants sécurisés sur le marché, tels que le U-Prove de Microsoft (http://research.microsoft.com/en-us/projects/u-prove/) et l'Identity Mixer de IBM (http://researcher.watson.ibm.com/researcher/view_project.php?id=664). Ces approches permettent au bénéficiaire de prouver certaines caractéristiques - telles que le fait qu'il a été reconnu et authentifié par une autorité crédible, qu'il a payé pour un certain droit ou service - sans divulguer d'informations personnelles ou de trace des transactions qui ont permis d'obtenir ces caractéristiques. Les parties utilisatrices ont une preuve cryptographique sécurisée que l'entité recevant ces identifiants sécurisés a l'approbation de l'autorité crédible, sans avoir besoin de savoir qui elle est ou comment elle a obtenu cette approbation.

Une telle technologie pourrait être utilisée pour établir un processus par lequel les entités menacées décrites ci-dessus pourraient obtenir un nom de domaine qui aura été enregistré en utilisant un identifiant protégé sécurisé. Ni le bureau d'enregistrement ni le validateur n'auraient des informations sur l'identité des entités menacées au-delà des contacts requis responsables du traitement des questions relatives au DNS. Ils ne seraient donc pas en mesure de répondre à des demandes d'informations personnelles ou d'adresses. Évidemment, il y a des soucis concernant la conformité technique, l'abus et la réduction de ces risques (développés ci-après). Le point principal est que pour les noms de domaine enregistrés en utilisation des identifiants sécurisés, les bureaux d'enregistrement et les registres n'assumeront plus le risque et la responsabilité quant à l'identification d'individus vulnérables à leurs agresseurs.

Questions opérationnelles

Afin d'éclaircir les questions et les risques associés à un tel service, l'EWG a examiné les situations potentielles suivantes :

1. Un requérant d'informations souhaite établir le vrai nom ou l'adresse d'un particulier tel que décrit aux points 2, 3 et 4 ci-dessus, pour ce qu'ils présentent comme des objectifs légitimes (allégations d'abus de marque de commerce, vente ou achat d'un nom de domaine, enquête sur la sécurité d'un produit, etc.). Il faudrait noter que dans des cas d'importance vitale, un bureau d'enregistrement se trouve dans une situation difficile lorsqu'il essaie de déterminer si le requérant agit sous de faux prétextes et on ne peut pas attendre du personnel qu'il comprenne à quel genre de menaces inconnues les personnes peuvent être confrontées, notamment dans les cas de changements d'identité.

2. Un requérant s'adresse au bureau d'enregistrement d'un nom de domaine (ou au validateur PBC désigné) alléguant une activité criminelle ou diffamatoire et demande le retrait d'un site Web utilisant ce nom de domaine. Dans ces situations, les conditions de service du bureau d'enregistrement et du fournisseur de services d'intermédiation seraient respectées et pourraient conduire à une requête de divulgation pour obtenir l'identité et l'adresse du détenteur de licence du nom de domaine. Toutefois, pour les noms de domaine enregistrés utilisant des identifiants sécurisés, une divulgation réussie conduit uniquement à l'autorité crédible qui a approuvé l'identifiant sécurisé. A partir de ce point, l'autorité crédible serait responsable de l'enquête concernant un abus potentiel du DNS. Dans certains cas, comme les activités criminelles, un retrait rapide peut être accordé à ces sites Web.

3. Dans les cas où des agences gouvernementales font des allégations selon lesquelles il y aurait discours politique au niveau de trahison ou autres affaires criminelles, les bureaux d'enregistrement peuvent être quand même forcés d'utiliser le retrait rapide de sites Web utilisant des noms de domaine enregistrés via des identifiants sécurisés, selon la loi pertinente dans la juridiction.

Même en prenant compte de ces restrictions, les identifiants sécurisés offriraient beaucoup plus de sécurité aux entités menacées que celle dont elles bénéficient actuellement. Et si le nouveau RDS nécessitera une exactitude de données et une responsabilité accrues, alors un tel service est requis. Pour ce faire, les fonctions principales suivantes devraient être développées :

1. Un processus pour établir par le biais de l'élaboration de politiques des critères concernant l'éligibilité des entités menacées à des identifiants sécurisés, en commençant par les exemples d'utilisateurs cités ci-dessus et d'autres que la communauté de l'ICANN considère appropriés.
2. Des formulaires de demandes, des attestations requises et des systèmes financiers, tous focalisés sur la garantie que les identités des entités menacées (et, dans certains cas, leurs certifiants) sont protégées. Dans tout système anonyme, c'est l'un des points faibles principaux.
3. Un conseil de révision indépendant pour évaluer et approuver les demandes d'identifiants sécurisés et les attestations de parties crédibles, tels que les gouvernements qui ont autorisé les changements de noms, les organisations des Nations Unies impliquées dans la protection des réfugiés, les associations internationales de journalistes, etc.
4. Les parties crédibles (telles que celles énumérées au point 3 ci-haut) prêtes à relayer des demandes d'identifiants sécurisés et les noms de domaines résultant de ce conseil de révision indépendant. Ces parties crédibles - dénommées ci-après destinataires d'identifiants sécurisés - doivent attester le besoin d'anonymat de l'entité menacée et assumer la responsabilité en cas d'abus potentiel du DNS de la part de noms de domaine enregistrés par identifiant sécurisé.
5. Les fournisseurs de services d'intermédiation accrédités qui seraient disposés à accepter des identifiants sécurisés lors de l'enregistrement de noms de domaine recevant une licence de l'approbateur d'identifiants sécurisés, ainsi que les systèmes financiers pour qu'ils puissent être payés.
6. Les politiques entourant les procédures de retrait rapide et autres atténuations d'abus du DNS. Ceci pourrait inclure un suivi de sécurité renforcée des noms de domaine enregistrés avec identifiants sécurisés, afin de réduire les risques de mauvaise utilisation du DNS et d'abus et afin d'aider à protéger les noms de domaine contre les attaques. Les parties alléguant un abus du DNS présenteraient leurs arguments au conseil qui a approuvé la demande de l'entité menacée ; l'approbateur d'identifiants sécurisés évaluerait l'abus allégué.

La figure suivante illustre les relations possibles entre ces parties, leurs responsabilités et le flux de communication entre elles.

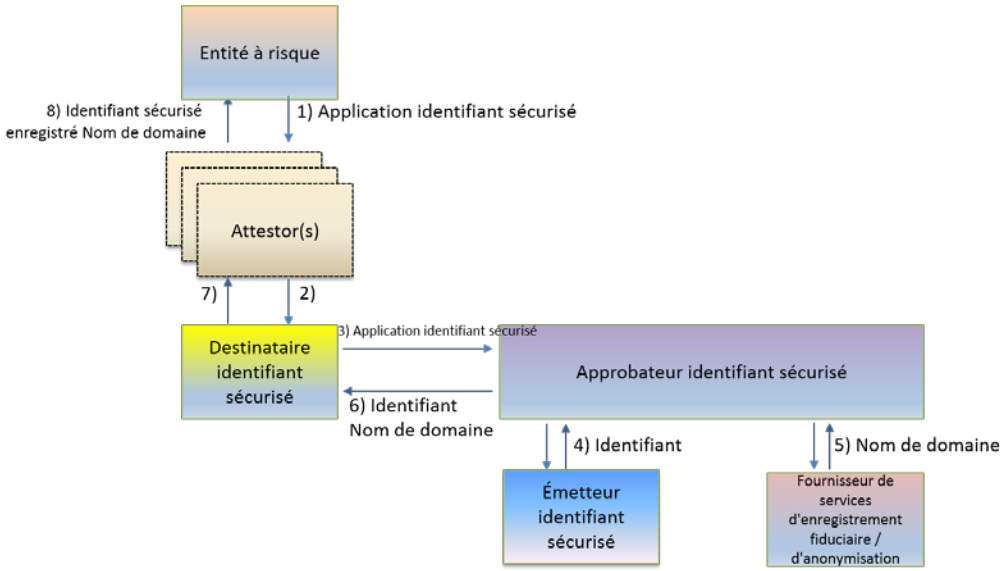


Figure 8. Modèle d'identifiants sécurisés et protégés

Risques résiduels

Les identifiants sécurisés ne sont pas largement utilisés parce que, entre autres raisons, ils sont compliqués à mettre en œuvre, notamment en ce qui concerne l'enregistrement et la révocation. Il a été soutenu que toutes les parties devraient être éligibles à un tel enregistrement, mais étant donné le seuil de travail requis pour établir ce service et s'assurer qu'il n'est pas utilisé à des fins frauduleuses ou criminelles, l'EWG considère cette approche irréalisable. L'EWG recommande que les identifiants protégés sécurisés soit développés pour un usage limité et après s'être assuré que les entités utilisant le service ont réellement un besoin légitime d'anonymat.

Il est aussi reconnu qu'une fois le nom de domaine enregistré et le site Web l'utilisant devenu opérationnel, des métadonnées de trafic Internet et des contenus de diverses natures peuvent conduire à l'identification de l'utilisateur du nom de domaine. Ceci dépasse le champ des préoccupations de l'ICANN qui se concentre uniquement sur les questions d'enregistrement de domaine et des données y associées, collectées, utilisées et divulguées afin de satisfaire les objectifs définis dans le cadre du mandat de l'ICANN. Les informations générées par l'utilisation du nom de domaine doivent être de la responsabilité des entités demandant et utilisant des noms de domaine enregistrés par identifiant sécurisé et il peut être important de fournir des informations soulignant ce risque. La responsabilité de l'ICANN prend fin avec le système même du nom de domaine.

Nº.	Principes relatifs aux identifiants protégés sécurisés
150.	Les particuliers et les groupes qui peuvent démontrer qu'ils pourraient encourir des risques s'ils étaient identifiés doivent pouvoir faire une demande anonyme et recevoir des noms de domaine enregistrés en utilisant des identifiants sécurisés, aidées par des validateurs et des tierces parties crédibles afin de fournir une protection entre les entités à risque et les bureaux d'enregistrement/validateurs.
151.	L'ICANN doit faciliter l'établissement d'un conseil de révision crédible indépendant qui validera les réclamations concernant les organisations à risque ou les particuliers afin d'approuver (et révoquer si nécessaire) les identifiants. Une telle organisation - ici dénommée approbateur d'identifiants sécurisés (SCA) - pourrait développer d'autres services, tels que l'éducation des utilisateurs concernant les risques et les pratiques sûres sur Internet.
152.	L'ICANN doit faciliter la mise en place ou l'octroi de licence à un émetteur d'identifiants sécurisés qui reconnaisse les approbations SCA et produise les identifiants sécurisés correspondants.
153.	L'approbateur d'identifiants sécurisés doit utiliser les identifiants sécurisés émis pour l'octroi de licence de nom de domaine des fournisseurs de services d'intermédiation accrédités comme d'habitude. Les informations du fournisseur de services d'intermédiation apparaîtront dans le RDS. Aucune des données de l'entité menacés utilisant le nom de domaine enregistré par identifiant sécurisé ne serait connue du RDS, et un système de paiement anonyme ou par intermédiation devra être utilisé.
154.	Les noms de domaine enregistrés utilisant des identifiants protégés sécurisés doivent suivre les procédures régulières de divulgation et de retrait des fournisseurs de services d'anonymisation/d'intermédiation accrédités. L'absence de réponse de la part d'un client de services P/P (à savoir, l'approbateur d'identifiants sécurisés) de manière opportune, ou la preuve d'abus du DNS pourraient résulter en un retrait rapide des noms de domaine enregistrés par identifiant sécurisé.
155.	Reconnaissant le fait que les noms de domaine enregistrés utilisant des identifiants protégés sécurisés puissent encourir eux-mêmes des risques d'attaques informatiques ou que les enquêtes d'infractions seraient difficiles, un

Nº.	Principes relatifs aux identifiants protégés sécurisés
	suivi de haute sécurité de ces noms de domaine pourrait être envisagé afin d'atténuer le risque.
156.	Des politiques et des processus doivent être établis pour l'approbation et la révocation de demandes d'identifiants protégés sécurisés. • Le processus d'approbation doit permettre à des certifiants de protéger suffisamment l'identité et la position géographique de l'entité menacée du destinataire d'identifiant sécurisé crédible qui présente la demande au SCA. Le nombre et l'identité des certifiants est transparent au RDS ; la seule partie ayant un interface direct avec le SCA est le destinataire d'identifiant sécurisé. • Le processus de révocation doit permettre une protection similaire de l'identité et de la position géographique d'un particulier menacé lors de l'application des conditions de service relatives aux identifiants sécurisés. Le SCA doit être tenu d'enquêter en cas d'allégations d'abus du DNS impliquant des identifiants sécurisés et d'imposer les conditions de service. Dans le cas d'abus du DNS assez grave pour dicter une révocation d'identifiant, le SCA tiendra le destinataire de l'identifiant sécurisé pour responsable.

c. Résumé des principaux avantages en matière de confidentialité

Avec des améliorations en termes d'exactitude et de responsabilité, il sera encore plus important de protéger les citoyens, notamment les vulnérables. Incorporer des principes et des mécanismes de protection des données, de services P/P accrédités et d'identifiants protégés sécurisés comme partie intégrante du RDS de nouvelle génération améliorera la confidentialité pour les titulaires de noms de domaine et les contacts.

Les principes de protection des données recommandés par l'EWG :

- Protègeraient de manière plus uniforme les données personnelles en appliquant une seule politique RDS harmonisée, mise en œuvre de manière cohérente dans l'écosystème du RDS et utilisant un « moteur de règles » pour appliquer la loi locale.
- Nécessiteraient moins que les données d'enregistrement et de contact soient publiques et anonymement disponibles.

- Protègeraient mieux les données du titulaire du nom de domaine et des contacts contre la mauvaise utilisation.

Les principes recommandés par l'EWG pour les fournisseurs de services d'anonymisation/d'intermédiation accrédités :

- Offriraient une plus grande clarté aux titulaires de noms de domaine à la rechercher de services d'anonymisation/d'intermédiation en établissant un cadre d'accréditation pour les fournisseurs de tels services.
- Nécessiteraient l'identification du nom de domaine comme ayant été enregistré par le biais de services offerts par un fournisseur d'anonymisation/d'intermédiation accrédité.
- Indiqueraient clairement dans les données d'enregistrement comment contacter ce fournisseur.
- Empêcheraient les parties tierces d'utiliser les données de contact du fournisseur d'anonymisation/d'intermédiation sans autorisation.
- Nécessiteraient un fournisseur d'anonymisation/d'intermédiation accrédité pour relayer les courriels au titulaire du ND sous-jacent et répondre aux demandes.
- Offriraient des attentes plus cohérentes et prévisibles aux représentants de la loi et autres tiers qui signalent les abus et demandent une divulgation.

Les principes relatifs aux identifiants protégés sécurisés recommandés par l'EWG :

- Établiraient pour la première fois des procédures permettant aux groupes vulnérables et défavorisés de bénéficier des avantages multiples d'avoir leurs propres domaines sur Internet.
- Protègeraient ceux qui ont le plus besoin d'utiliser Internet à des fins de liberté de parole et de communication au sein des groupes, tout en offrant des recours en cas d'abus.
- Soustrairaient la responsabilité potentielle aux validateurs et bureaux d'enregistrement aujourd'hui responsables en cas de divulgation d'informations personnelles hautement sensibles suite à des tentatives de manipulation sociale.
- Offriraient une sécurité supplémentaire aux noms de domaine enregistrés utilisant des identifiants protégés sécurisés.
- Exigeraient un retrait rapide des sites Web enregistrés via identifiants protégés sécurisés impliqués dans une mauvaise utilisation du DNS.

VIII. Modèles de RDS possibles

a. Principes de conception des modèles

Le présent rapport fournit des détails concernant plusieurs modèles alternatifs examinés par l'EWG, avec une analyse de la manière selon laquelle ces modèles pourraient satisfaire les principes recommandés par l'EWG. Tous les modèles ont été évalués en utilisant des critères pluriels tels qu'identifiés à l'annexe F.

En effectuant cette analyse, lEWG a appliqué les principes de conception suivants :

Nº.	Principes de conception des modèles
157.	**Collecte :** Aujourd'hui, les bureaux d'enregistrement ou les affiliés des bureaux d'enregistrement collectent et stockent des informations d'enregistrement pour leurs propres clients (les titulaires des noms de domaine). Ce processus est distribué de manière intrinsèque. En plus de continuer à collecter des données d'enregistrement des titulaires par les bureaux d'enregistrement ou leurs affiliés, l'EWG propose la collecte de données de contact par les validateurs.
158.	**Stockage :** De multiples modèles possibles existent pour le stockage des informations d'enregistrement à travers tous les gTLD. L'EWG a identifié plusieurs modèles possibles, en a localisé deux qui semblent être les plus indiqués et choisi un modèle recommandé en appliquant les critères d'évaluation reflétés à l'annexe F**.**
159.	**Accès :** Afin de protéger la vie privée du sujet des données, une interface centralisée doit permettre aux requérants appropriés d'avoir accès aux informations d'enregistrement à travers tous les gTLD, y compris un accès non-authentifié aux données publiques et un accès authentifié aux données sécurisées pour les utilisateurs accrédités.
160.	**Protocole :** Le RDS doit utiliser le RDAP[33] ou le protocole EPP (tel qu'approprié pour chaque interface) comme protocole sous-jacent d'accès aux annuaires afin d'obtenir des informations d'enregistrement à partir des emplacements de stockage, où qu'ils soient.

[33] http://tools.ietf.org/html/draft-ietf-weirds-rdap-query-02

b. Les modèles considérés

Afin de tester les modèles de systèmes alternatifs considérés par l'EWG dans son rapport initial et les modèles supplémentaires suggérés par la communauté de l'ICANN, l'EWG a d'abord déterminé quels modèles devaient être examinés de manière approfondie. Chacun de ces modèles diffère des autres de manière variée, y compris comment les informations d'enregistrement sont copiées ou demandées via le RDS. Ces différences sont résumées dans le tableau ci-dessous[34] et expliquées plus en détail à l'annexe F.

MODÈLES POSSIBLES	Collecte	Stockage	Copie	Accès
WHOIS actuel	RR	RR/Ry	N/D	RR/Ry
Fédéré	RR & V	RR/Ry & V	N/D	RDS
Synchronisé *	RR & V	RR/Ry & V	RDS	RDS
Régional	RR & V	RR/Ry & V	Régional	RDS
Dérogation	RR & V	RR/Ry & V	Facultatif	RDS
Contournement	RR & V	RR & V	RDS	RDS

*** Note :** Le modèle précédemment mentionné comme **« RDS globalisé (ARDS) »** a été renommé **« RDS synchronisé (SRDS) »** pour mieux refléter la propriété de ce modèle consistant à utiliser des données localisées dans de multiples endroits de manière cohérente et coordonnée. TOUS les modèles considérés ici seraient déployés en utilisant les meilleures pratiques pour parvenir à une tolérance de panne, une disponibilité élevée et un équilibre de charge, y compris des centres de données diversifiés du point de vue géographique, une connectivité diverse robuste et une infrastructure redondante à chaque centre de données.

c. Modèle recommandé

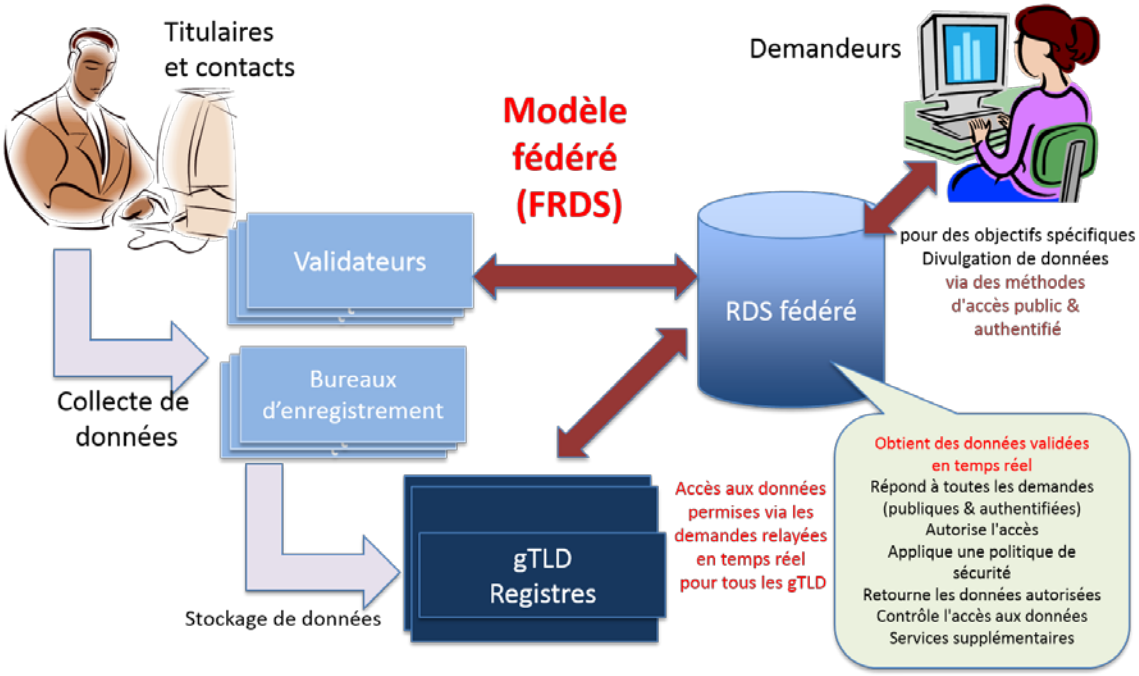
Les modèles de systèmes possibles identifiés ci-dessus diffèrent dans le sens où les informations d'enregistrement sont copiées au RDS ou demandées via le RDS. L'EWG a soigneusement examiné chaque modèle pour déterminer la manière selon laquelle ces différences pourraient avoir un impact sur les divers attributs. Après la comparaison de

[34] Clé pour le tableau récapitulatif des modèles : RR se réfère aux bureaux d'enregistrement, Ry se réfère au registres, V se réfère aux validateurs

ces modèles possibles, l'EWG a trouvé que, sauf pour l'actuel WHOIS, ils sont tous capables de satisfaire dans une certaine mesure les principes RDS recommandés par l'EWG. Parmi ceux-ci, l'EWG s'est concentré sur les deux modèles les plus prometteurs pour un examen plus approfondi, le modèle fédéré et le modèle synchronisé (anciennement connus sous le nom de « modèle intégré »), **et a finalement recommandé le modèle synchronisé (SRDS)**.

Modèle fédéré (deuxième choix)

Ce modèle décrit un RDS qui ire des informations d'enregistrement de zones de stockage distribuées opérées par des registres épais et des validateurs qui utilisent tous un schéma de données commun fédéré. Il n'y a pas d'agrégation de données dans un seul lieu de stockage mais plutôt un accès unifié public/sécurisé à travers le RDS à des informations d'enregistrement obtenues en temps réel de tous les registres gTLD (données de noms de domaine) et validateurs (coordonnée de contact).



Dans ce modèle, les données sont tirées par le FRDS des validateurs et des bureaux d'enregistrement/registres via RDAP. Le flux de données de contact et d'enregistrement associé à ce modèle est décrit en détail à l'annexe I (schémas opérationnels du RDS) et illustré à l'annexe E en utilisant des exemples de requêtes.

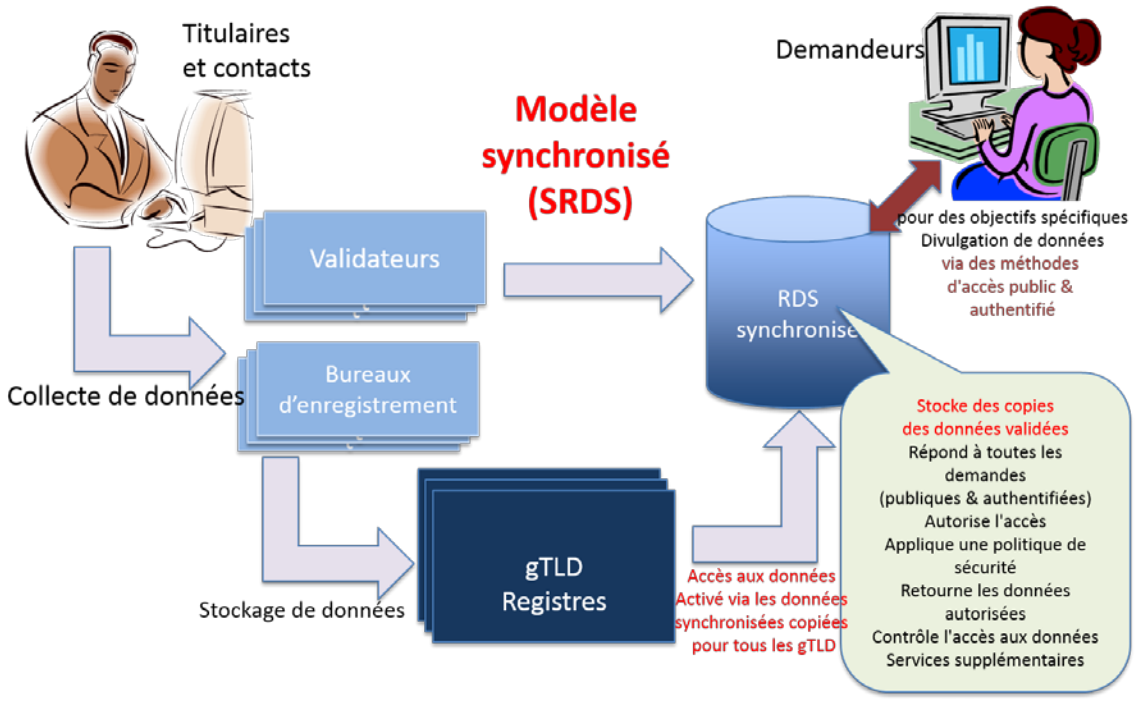
Modèle synchronisé (SRDS) (recommandé)

Ce modèle décrit un RDS qui, presque en temps réel, copie des données reçues des zones de stockage distribuées opérées par des registres épais et validateurs dans un

système synchronisé qui agrège et entrepose les données dans une architecture distribuée opérée par le RDS.

Dans ce modèle, le RDS est la source de données faisant autorité qui fournit un accès autorisé, tel que décrit. Ainsi, le RDS dépasserait l'exigence actuelle (et le besoin actuel) du RAA en termes d'intemporalité des actualisations des bureaux d'enregistrement et des registres. Les registres, les bureaux d'enregistrement et les validateurs peuvent fournir aux clients un accès à leurs propres données mais toutes les demandes d'accès sécurisé doivent trouver une réponse en interrogeant le RDS. Ce modèle est adapté aux recommandations précédentes du WHOIS et aux demandes de réduction de la confusion des consommateurs concernant le lieu et les modalités d'accès aux données d'enregistrement. Il minimise aussi les exigences de coût et de responsabilité pour les bureaux d'enregistrement et les registres.

Bien que le RDS fournisse un accès aux données, les données ne sont pas entreposées dans un seul lieu mais plutôt dans de multiples positions, diversifiées et redondantes selon les meilleures pratiques pour les systèmes qui nécessitent une tolérance des fautes, une disponibilité élevée et un équilibrage des charges. Les registres et les validateurs continuent à entreposer leurs propres données, mais le RDS peut utiliser des copies synchronisées de ces données afin de traiter les requêtes d'accès de manière plus efficace.



Dans ce modèle, les données sont transmises au SRDS par des validateurs et des bureaux d'enregistrement/registres via EPP. Le flux de données de contact et

d'enregistrement associé à ce modèle est décrit en détail à l'annexe I (schémas opérationnels du RDS) et illustré à l'annexe E en utilisant des exemples de requêtes. Vous trouverez ci-dessous une comparaison relative de ces deux modèles préférés par l'EWG, après application de la méthodologie identifiée à l'annexe F.

- **Incidences sur la sécurité** - les deux modèles produisent des résultats similaires lorsqu'ils sont évalués en termes d'impact sur la sécurité. Bien qu'il y ait eu des commentaires publics selon lesquels un modèle globalisé (renommé par la suite synchronisé) comme celui suggéré dans le rapport initial poserait un risque dû à un « point de défaillance unique » à partir d'une interface centralisée, l'EWG a trouvé que ceci n'était différent des risques posés aujourd'hui par des grands registres de gTLD et des sites Web Internet d'envergure mondiale. Les bonnes pratiques actuelles exigent que de grands systèmes basés sur informations utilisent de multiples centres de données, des systèmes de stockage de sauvegarde et de reprise après une catastrophe, ainsi qu'une infrastructure diversifiée du point de vue géographique et pleinement redondante afin d'atténuer ces risques.

  Un modèle synchronisé présente l'avantage ajouté d'être mieux en mesure d'assurer la mise en œuvre de sécurité et l'application de politiques. En exploitant de manière rigoureuse les composantes du système, un modèle synchronisé avec une architecture distribuée qui est gérée par un opérateur produirait probablement une approche plus uniforme pour atteindre les objectifs de sécurité en comparaison avec le modèle fédéré. Ceci est en partie dû au fait que dans un modèle fédéré, des milliers de registres, de bureaux d'enregistrement et de validateurs gèreraient leurs bases de données respectives en ayant des niveaux différents d'expertise et d'investissement dans les pratiques de sécurité.

- **Préoccupations juridictionnelles et de confidentialité** - les deux modèles produisent des résultats similaires lors de l'évaluation des impacts juridictionnels et de confidentialité. Dans le modèle fédéré, les données sont stockées et contrôlées au niveau du bureau d'enregistrement avec des copies supplémentaires gardées dans d'autres lieux (notamment, celui d'un bureau d'enregistrement, d'un validateur et de centres de sauvegarde des données de par le monde). Le modèle synchronisé stocke et contrôle les données dans de multiples lieux séparés de ceux des registres, avec des copies supplémentaires gardées dans d'autres lieux (bureau d'enregistrement, registre, validateur et centres de sauvegarde de données situés de par le monde). Lorsque nous avons examiné tous les modèles évalués, nous avons vu que la plupart n'éliminaient pas le transfert de données vers de multiples lieux, sauf

pour le « modèle de contournement » qui élimine le besoin pour les registres de stocker les données de contact.

En outre, le modèle synchronisé permet une application plus cohérente des règles pour se conformer aux exigences de vie privée locales, puisqu'il est plus facile de gérer les règles administrées par une entité (l'opérateur du RDS synchronisé) que par un éventuel millier ou plus de participants dans un modèle fédéré.

- **Accréditation** - l'application des exigences d'accréditation est possible dans les deux modèles synchronisé et fédéré. Les deux modèles peuvent offrir des attributs permettant de débusquer et d'arrêter ceux qui abusent du système d'accréditation, bien qu'il puisse être plus facile de le faire lorsque la base de données est gérée par une seule entité dans un modèle synchronisé en comparaison avec un éventuel millier ou plus de participants dans le modèle fédéré. De plus, la mise en oeuvre d'un modèle fédéré nécessiterait des dépenses supplémentaires ainsi que des obligations contractuelles détaillées, des accords de niveaux de service et une supervision du département de conformité de l'ICANN pour soutenir des capacités cohérentes d'application et d'audit.

- **Exploitation** - le modèle synchronisé offre des efficacités dans certains domaines opérationnels qu'il est difficile d'obtenir dans un modèle fédéré. Par exemple, déployer un portail convivial qui affiche des données dans de multiples langues/écritures pourrait être plus facile dans le modèle synchronisé où les données de contact pourraient être traduites ou translittérées dans un format plus cohérent. Pour obtenir une cohérence similaire dans un modèle fédéré, les accords auraient besoin de spécifications et de normes de traduction et de translittération clairement articulées. Les deux modèles peuvent être conçus pour permettre des audits aléatoires de qualité des données, bien que ceci soit probablement plus facile à accomplir dans un modèle synchronisé.

  Les préoccupations de temps d'attente et de synchronisation des données sont réduites dans un modèle fédéré, puisque les données à afficher proviennent directement du registre même. Cependant, tirer des données d'un modèle synchronisé introduit des questions d'attente qui peuvent être résolues en faisant les validateurs et les bureaux d'enregistrement (via les registres) transmettre en temps opportun les actualisations EPP au SRDS (voir principe de conformité #108).

- **Mise en œuvre** - un modèle fédéré s'aligne de manière plus étroite sur le modèle distribué du WHOIS actuel qu'un modèle synchronisé. Toutefois, les exigences de

performance et les capacités de recherche nécessaires pour fournir les attributs robustes recommandés par l'EWG nécessiteraient des spécifications détaillées et des critères de mesure de la performance qui dépassent de loin ceux offerts aujourd'hui par le WHOIS. Une supervision plus importante de la part du département de conformité de l'ICANN et des ressources plus importantes seraient nécessaires pour s'assurer que toutes les parties dans le système fédéré ont des performances au niveau prévu. Dans les deux modèles, les participants concernés auraient besoin d'actualiser leur plateforme de logiciel pour interagir avec l'interface du RDS et recevoir les résultats de recherche et les données de contact requis.

- **Coûts** - il pourrait y avoir des économies de coûts réalisées par les bureaux d'enregistrement et les registres (ainsi que les validateurs) dans le modèle synchronisé en étant libéré du fardeau opérationnel consistant à répondre constamment à des demandes complexes provenant de l'interface du RDS (telles que les requêtes inverses) qui serait requis dans un modèle fédéré. En particulier, la comparaison des coûts des modèles (décrite en détail à l'annexe F) a conduit aux conclusions suivantes :

  (1) Avec les hypothèses utilisées, le système RDS central est légèrement moins cher dans le modèle RDS fédéré (FRDS) que dans le modèle RDS synchronisé (SRDS). Toutefois, le modèle fédéré est hautement sensible au nombre de requêtes inverses. **Avec un plus grand nombre de requêtes inverses, le modèle FRDS devient sensiblement plus cher que le SRDS.** Par exemple, avec 3% de charge de requêtes inverses au lieu de 1% de charge de requêtes inverses, le coût du modèle FRDS devient 35% plus cher que le modèle SRDS. Avec 5% de requêtes inverses, le coût global du FRDS augmenterait d'environ 85%. Il s'agit d'un facteur d'incertitude et de risque important associé au modèle FRDS. Le modèle SRDS est estimé moins sensible au nombre de requêtes inverses.

  (2) De plus, **le modèle FRDS a un coût plus élevé sur l'ensemble de l'écosystème à cause de son impact [de coût plus élevé] sur les opérateurs de registres**. Dans le modèle FRDS, chaque opérateur de registre devrait mettre en œuvre et soutenir - selon le SLA - des réponses à des requêtes RDAP RDS en temps réel, y compris les requêtes inverses et les requêtes historiques WhoWas. Pour ces dernières, les données historiques devraient également être maintenues par les opérateurs de registres, augmentant encore plus le coût pour les registres. Il faudrait noter que ce coût supplémentaire par registre serait supérieur et au-delà de l'impact du système central RDS estimé ci-dessus.

(3) En outre, le modèle FRDS nécessiterait des opérations d'application et des efforts de soutien, de maintenance et d'essais plus importants en comparaison avec le modèle SRDS, puisqu'il y aurait de plus grandes interactions avec les opérateurs de registres.

De plus amples détails sur l'analyse de coût de ce modèle, son champ et sa méthodologie ainsi que les hypothèses et données volumétriques sous-jacentes se trouvent à l'annexe F et dans « *l'analyse de coût du modèle de mise en œuvre du service d'annuaire d'enregistrement (RDS)*[35] » préparée pour l'ICANN par IBM en mars 2014.

d. Principes relatifs au stockage, au dépôt fiduciaire et à l'inscription .

Nº.	Exigences communes pour le stockage, le dépôt fiduciaire et l'inscription
161.	Des politiques relatives au lieu, au maintien, à la confidentialité et à l'accès doivent être élaborées.
162.	Les politiques et mises en œuvre du stockage, du dépôt fiduciaire et de la connexion doivent être conformes aux lois locales et internationales.
	Principes de stockage
163.	Pour maintenir les systèmes redondants et éliminer les points de contact uniques de défaillance, les données doivent être logées dans différents sites (par ex. validateur, bureau d'enregistrement, registre, fournisseur de dépôt et fournisseur RDS).
164.	Il doit y avoir cohérence lorsque les données sont logées dans de multiples sites.
165.	Le RDS doit maintenir les éléments de données en toute sécurité de sorte à protéger la confidentialité et l'intégrité des éléments de données exposées au risque d'utilisation ou de divulgation non autorisée.
166.	Les données de transaction doivent être stockées pour une durée indéterminée afin de maintenir un état précis des changements de données au fil du temps et soutenir la fonctionnalité WhoWas, mais pas plus longtemps que les limites (le cas échéant) requises pour la conformité aux lois régissant la protection des données. Les coordonnées de contacts orphelins devraient aussi être régulièrement effacées, conformément aux lois (par ex. un an après la dissociation).

[35] https://community.icann.org/display/WG/EWG+Public+Research+Page

	Principes relatifs au dépôt fiduciaire[36]
167.	Les audits doivent être réalisés sur les données déposées afin de vérifier qu'elles soient complètes, tester leur format et leur intégrité.
168.	Le dépôt et l'audit de données déposées peut être plus facile à coordonner avec un modèle de RDS synchronisé.
169.	Les données déposées doivent être elles-mêmes cryptées et opaques pour les contrôleurs.
170.	Les données déposées doivent être maintenues pendant une période de temps alignée sur les exigences de l'accord d'accréditation de bureau d'enregistrement, les accords individuels de registres gTLD et les lois en vigueur sur la protection des données. Actuellement, ceci serait pour la durée du parrainage des données par l'entité de publication et pour une période de deux années supplémentaires par la suite ou plus longtemps si requis par l'accord de registre gTLD mais pas plus longtemps que la durée maximum prévue par la loi.
	Principes d'inscription
171.	Les demandes au RDS doivent être inscrites pour avoir un compte-rendu de la façon dont le système est utilisé.
172.	On pourrait avoir besoin du journal des inscriptions pour détecter des abus visant les systèmes distribués.
173.	Les changements doivent être inscrits pour fournir un historique des éléments de données au fil du temps.
174.	L'accès aux journaux opérationnels du RDS doit être réservé aux individus et entités de confiance, authentifiés et autorisés ayant un objectif spécifique et un « besoin de savoir ». Ceci doit inclure les opérateurs autorisés du RDS même (pour confirmer et régler les problèmes opérationnels du RDS) et les entités autorisées du secteur de protection des données (pour surveiller la conformité du RDS à la législation sur la protection des données). (Voir aussi section VIII(b), accès aux représentants de la loi).

[36] Le dépôt fiduciaire se réfère à un système crypté de sauvegarde auprès d'un tiers de confiance dans le cas de catastrophes, de défaillance du système, etc. Se référer au RAA pour plus de détails.

IX. Coûts et impacts

a. Principes relatifs au coût

Tel qu'indiqué à l'annexe F, méthodologie pour la comparaison des modèles, l'EWG a aussi considéré les coûts et impacts du RDS. L'EWG reconnait que certains aspects du modèle recommandé puissent induire de nouveaux coûts, mais il estime que de nombreux frais cachés encourus compte tenu du système actuel inefficace et trop souvent inexact du WHOIS seront réduits. A mesure que le RDS recommandé délivrera de nouveaux services améliorés, les bénéfices et les coûts doivent être évalués. L'approche recommandée fournira pour la première fois aux faiseurs de politiques l'option d'établir des moyens pour les requérants de données d'enregistrement du système qui contribuent de manière efficace à l'opération de ce système.

Les coûts d'exploitation du WHOIS sont inconnus aujourd'hui, mais ils comprennent des coûts assumés par l'ensemble de l'écosystème et non seulement par les registres et les bureaux d'enregistrement qui offrent des services WHOIS. Les bureaux d'enregistrement ne sont pas tenus de ventiler les coûts du WHOIS et peuvent avoir des difficultés à faire la distinction parmi les coûts de fourniture de tels services pour les gTLD en comparaison avec les ccTLD. D'autres acteurs de l'écosystème encourent des frais résultant des inefficacités et des insuffisances du WHOIS actuel, à savoir les détenteurs de marques de commerce qui paient pour les services d'entreprises de protection des marques et de services commerciaux WHOIS afin d'identifier les cybersquatteurs.

L'EWG recommande les principes suivants relatifs au coût :

Nº.	Principes relatifs au coût
175.	L'accès non authentifié (non sécurisé) aux éléments de données publics doit être gratuit.
176.	L'accès authentifié (sécurisé) des représentants de la loi aux éléments de données autorisés (sous réserve de la procédure adéquate) doit faire l'objet d'un coût spécial.
177.	La conception du RDS devrait aspirer à la rentabilité et la minimisation des coûts sans compromettre les autres buts.
178.	Le RDS devrait fonctionner sur un modèle de recouvrement des coûts.
179.	Pour faciliter la migration du WHOIS, une plateforme de développement de logiciel RDS devrait être créée et financée par l'ICANN afin de minimiser les coûts de mise en œuvre pour les bureaux d'enregistrement/registres, validateurs et accréditeurs d'utilisateurs du RDS.

180.	La mise à disposition de cette plateforme de développement de logiciel ne devrait pas être indûment contraignante pour les autres utilisateurs du RDS.

Sans entrer dans les détails spécifiques de mise en œuvre, les coûts pourraient être partagés à travers l'écosystème. Des exemples où les coûts pourraient être recouvrés sans imposer des frais d'octroi de licence variés, selon l'utilisateur, les éléments de données faisant l'objet de l'accès ou l'objectif (tels que frais d'utilisation commerciale, frais d'inscription pour les utilisateurs intensifs ou frais d'accès privilégié) ou facturer des frais pour des services liés (tels que des frais d'octroi d'identifiant ou des frais de pré-validation).

Le RDS peut aussi produire des économies de coûts pour les registres et bureaux d'enregistrement desquels il n'est plus requis de fournir un accès public ou des niveaux de services stricts en matière de temps de réponse. Des économies de coûts peuvent aussi être réalisées pour les requérants à la recherche de données de par l'élimination des inefficacités dues aux fournisseurs non conformes (bureaux d,enregistrement, registres, validateurs ou fournisseurs de services d'anonymisation/d'intermédiation accrédités).

b. Avantages comparés au WHOIS actuel selon le RAA 2013

Les lacunes du WHOIS ont été documentées au cours des dix dernières années dans de nombreux rapports et études, mentionnés à l'annexe B. Des améliorations du WHOIS, reflétées dans le nouvel accord d'accréditation de bureau d'enregistrement de 2013 (RAA 2013), alliées à d'autres améliorations résultant de l'évaluation des recommandations de l'équipe de révision du WHOIS par le Conseil d'administration de l'ICANN ont résolu quelques insuffisances perçues dans le WHOIS.

Bien que le RAA 2013 ait introduit plusieurs nouvelles obligations, surtout les exigences de validation et de vérification pour améliorer l'exactitude, il existe encore d'autres lacunes significatives. Ces lacunes sont résumées ci-dessous, associées à des sections du présent rapport qui comprennent des recommandations permettant d'obtenir des avantages.

Lacunes du WHOIS selon le RAA 2013	abordées par le RDS dans la section
L'accès public anonyme à tous les éléments de données crée un environnement où l'atteinte et l'abus peuvent avoir lieu, avec peu de	III Utilisateurs/Objectifs IV Amélioration de la responsabilité

Lacunes du WHOIS selon le RAA 2013	abordées par le RDS dans la section
responsabilité ou d'aptitude à remédier	VI(d) Responsabilité et audit
Capacité limitée de protéger la vie privée des particuliers	VI(a) Protection des données VII Amélioration de la vie privée des titulaires de ND
Capacité limitée d'assurer l'intégrité des données d'enregistrement ; les titulaires de ND peuvent facilement fournir de fausses coordonnées de contact, y compris celles détenues par d'autres	V Amélioration de la qualité des données V(g) Capacité de données de contact uniques
Manque de dispositifs de sécurité	IV(b) Accès non authentifié et sécurisé aux données IV(c) Accréditation d'utilisateur du RDS
Manque de capacités d'audit	VI(d) Responsabilité et audit VIII(d) Stockage des données, dépôt fiduciaire et inscription
Accès non directement lié à des objectifs légitimes énoncés	III Utilisateurs/objectifs III(e) Contacts basés sur objectifs
Interfaces et réponses aux requêtes WHOIS incohérentes	IV(b) Accès non authentifié et sécurisé aux données VIII Modèles possibles de RDS
Pas de support ou de normes pour l'affichage de données d'enregistrement internationalisées	IV(b) Accès non authentifié et sécurisé aux données V(e) Interaction avec les validateurs
Capacité limitée d'appliquer des règles différentes pour se conformer aux régimes différents relatifs à la confidentialité des données	VI(a) Protection des données
Des niveaux d'exactitude inacceptables créent des inefficacités pour ceux souhaitant communiquer avec les titulaires de noms de domaine	V Amélioration de la qualité des données III(e) Contacts basés sur objectifs
Processus de gestion encombrants pour actualiser	V Amélioration de la qualité des

Lacunes du WHOIS selon le RAA 2013	abordées par le RDS dans la section
des contacts à travers de multiples noms de domaine	données V(c) Exactitude, audit et processus de restauration
Difficultés dans l'identification et la communication avec les clients des services d'anonymisation et d'intermédiation	III(e) Contacts basés sur objectifs VII(a) Services d'anonymisation/d'intermédiation Annex H Modèle de relais et de divulgation
Pas de règlementation des services d'anonymisation ou d'intermédiation, au-delà des exigences du RAA 2013 qui s'appliquent uniquement aux bureaux d'enregistrement et à leurs affiliés	VII(a) Services d'anonymisation/d'intermédiation Annex H Modèle de relais et de divulgation

c. Évaluation de risques et d'impact

Comme il est indiqué dans la section IV, amélioration de la responsabilité, l'EWG recommande la réalisation d'une évaluation des risques de champ étendu qui confirme que les principes du RDS recommandés dans ce document résultent en fait en une collecte appropriée et en une divulgation des données pour des objectifs définis, parvenant au bon équilibre entre les risques et les bénéfices.

Le 14 mars, l'EWG a invité toutes les parties qui fournissent ou utilisent des données d'enregistrement de noms de domaine gTLD à participer à une enquête en ligne sur les risques du RDS, y compris les titulaires de ND, les bureaux d'enregistrement, les registres et le vaste éventail de particuliers, d'entreprises et autres organisations consommatrices des données du WHOIS aujourd'hui. Cette enquête à offert aux participants l'occasion d'interpeller l'EWG à propos des risques et des bénéfices que le système de nouvelle génération visant à remplacer le WHOIS pourrait représenter pour eux.

Avant de finaliser le présent rapport, l'EWG a examiné l'instantané des risques et des bénéfices identifiés à travers cette enquête en espérant pouvoir réduire les risques imprévus et non nécessaires. Jusqu'au 29 mai 2014, la version anglaise de cette enquête avait recueilli 180 réponses partielles ; environ 100 ont complété l'enquête dans sa

totalité. A ce jour, les participants provenaient d'Amérique du nord (68%), d'Europe (35%), d'Asie (20%), d'Amérique Latine (14%), d'Afrique (11%) et d'Océanie (10%) et se répartissaient de manière égale entre ceux qui UTILISENT et ceux qui FOURNISSENT des données d'enregistrement. Les réponses ont éclairé les risques et bénéfices les plus probables et pouvant avoir une incidence sur les domaines suivants : technique, opérationnel, juridique et financier, sécurité et vie privée. Une douzaine de participants ont aussi commenté les risques inévitables et acceptables et les moyens de déplacer ou de réduire les risques.

Afin de permettre à la communauté étendue de contribuer à ce sujet, l'EWG a décidé de garder l'enquête sur les risques du RDS ouverte tout au long de juillet 2014 et de lancer des versions traduites. Les réponses seront utilisées pour guider la révision du présent rapport de la part du Conseil d'administration de l'ICANN et comme contribution à une analyse formelle future des coûts, risques et bénéfices pour toutes les parties prenantes qui seraient affectées par un remplacement du WHOIS par le RDS[37].

[37] Voir aussi l'évaluation des risques du DNS (1ère répétition) pour la consultation publique de l'ICANN

X. Conclusions et prochaines étapes

Après avoir considéré les points de vue de nombreuses parties prenantes dans l'écosystème qui dépendent des données d'enregistrement, l'EWG recommande à l'unanimité d'abandonner le modèle actuel du WHOIS - qui donne à chaque utilisateur le même accès public anonyme aux données d'enregistrement des gTLD - en faveur d'un système de remplacement, bâti en partant à zéro.

L'EWG estime que les principes et le RDS de nouvelle génération recommandés dans le présent rapport final apportent une base plus solide que celle qui existe aujourd'hui, une base à partir de laquelle on puisse protéger la vie privée et assurer une plus grande exactitude, responsabilité et transparence pour l'écosystème entier de l'ICANN pour les années à venir. Le RDS tire parti en allant bien au-delà des améliorations réalisées en vertu du RAA 2013 récemment négocié, tel que décrit de manière plus complète dans la section IX(b).

Bien que le rapport final puisse paraître trop détaillé pour certains, il n'est pas exhaustif. Comme nous le notons à l'annexe A, le rapport aborde chacune des questions posées par le Conseil. Cependant, plusieurs questions restent à aborder de manière plus complète à l'avenir - soit dans un processus suivant de développement de politique (PDP) soit dans des efforts de mise en œuvre connexes.

- **Organismes d'accréditation et politiques pour les communautés d'utilisateurs du RDS.** Comme des communautés d'utilisateurs spécifiques peuvent avoir accès à des données sécurisées pour un objectif approuvé, des politiques visant à identifier les personnes qualifiées en tant que membres de ces communautés devraient être examinées durant la phase de mise en œuvre, ainsi que des organismes d'accréditation et des modèles possibles appropriés pour chaque communauté.
- **Extensions requises vers les EPP et RDAP.** Comme décrit en détail à l'annexe G, l'EWG recommande que des protocoles standard soient utilisés pour soutenir les besoins du RDS, mais a identifié certaines extensions qui seraient requises pour soutenir pleinement le modèle RDS recommandé et les éléments de données.
- **Évaluation de risques et d'impact.** Comme décrit dans la section IX, l'EWG recommande qu'une évaluation complète des risques et une analyse des coûts/bénéfices soient entreprises avant la mise en œuvre du RDS recommandé et a déjà lancé une enquête pour recueillir des contributions relatives à ce processus.
- **Politique de confidentialité du RDS.** Comme décrit dans la section VII, l'EWG recommande qu'une politique de de confidentialité pour le RDS soit établie par l'ICANN et basée sur les bonnes pratiques standard relatives à la protection de la vie

privée et que des clauses contractuelles standard soient élaborées mettant en vigueur cette politique dans l'écosystème du RDS.

- **Traduction/translittération des données de contact.** Comme il existe déjà un processus de développement de politique (PDP) en cours concernant cette question, l'EWG a choisi d'éviter la duplication des efforts au-delà des principes identifiés dans la section IV(b), et suggère plutôt que le résultat du PDP en cours soit examiné dans le futur pour déterminer comment appliquer de nouvelles politiques au RDS.
- **Services d'anonymisation et d'intermédiation.** Les principes de l'EWG ayant rapport avec les fournisseurs d'anonymisation/d'intermédiation accrédités auront besoin d'être pris en considération en combinaison avec le travail actuellement en cours dans la GNSO à ce sujet, alliant le résultat du PDP actuel avec toute mise en œuvre du RDS.
- **Écosystème de validateurs.** La création d'un programme d'accréditation pour les validateurs, et les processus utilisés pour validet les coordonnées de contact des titulaires de noms de domaine et des contacts situés de par le monde, auront besoin d'être examinés de manière plus approfondie pendant la phase de mise en œuvre.

Le RDS reflète avec attention les compromis équilibrés et réalisés avec des éléments inter-dépendants qui ne devraient pas être séparés. Ces compromis tsont guidés par les contributions reçus par l'EWG des nombreux commentaires publics, des webinaires et des consultations sur son travail à ce jour. Par conséquent, l'EWG encourage le Conseil à transmettre le rapport final à la GNSO afin qu'il soit adopté dans son ensemble. Choisir d'adopter certains mais pas tous ces principes de conception du RDS réduit les bénéfices pour l'écosystème entier. L'EWG s'inquiète du fait que l'examen des composantes séparément puisse conduire à une réitération de la dissension et de l'impasse dans la communauté qui ont accompagné les tentatives précédentes d'amélioration du WHOIS.

L'EWG a remis ce rapport final au président-directeur général de l'ICANN et au Conseil d'administration, l'a mis en ligne, et a organisé de multiples sessions lors de la réunion de l'ICANN de juin 2014 à Londres. Il conduira également des webinaires et prévoira d'autres occasions de discuter du rapport et de répondre aux questions de la communauté de l'ICANN à cet égard. Le rapport final est destiné à servir de fondement pour le processus de développement de politiques de la GNSO demandé par le Conseil pour les dispositions des données d'enregistrement des gTLD et pour des négociations contractuelles, selon le cas. Durant l'examen du présent rapport final par le Conseil d'administration et la communauté de l'ICANN, l'EWG recommande que la prise en considération soit encadrée par les questions suivantes :

- Est-ce que le RDS est préférable à l'actuel WHOIS ?

- Si la réponse est non, est-ce que la communauté de l'ICANN est d'accord avec le fait que le système WHOIS actuel devrait continuer, et qu'il peut répondre aux besoins de l'Internet mondial en évolution ?

L'EWG est certain que le présent rapport final répond aux directives du Conseil d'administration de l'ICANN pour aider à redéfinir l'objectif et les dispositions en matière de données d'enregistrement des gTLD et fournira une base solide pour aider la communauté de l'ICANN (à travers l'organisation de soutien des noms génériques, GNSO) à créer une nouvelle politique mondiale pour les services d'annuaire gTLD.

ANNEXE A : REPONSE AUX QUESTIONS DU CONSEIL

La résolution du Conseil d'administration qui a ordonné le travail de l'EWG comprenait une série de questions spécifiques devant être répondues dans le cadre de l'analyse de l'EWG. La présente annexe référence les sections du présent rapport qui aborde les préoccupations du Conseil.

Questions et orientations du Conseil	Sections du rapport
L'EWG doit redéfinir l'objectif de : • la collecte, • du maintien et • de la fourniture d'un accès aux données d'enregistrement de gTLD et • considérer des protections pour les données	Section III, utilisateurs et objectifs Section VI, améliorer la responsabilité
Pourquoi les données sont-elles collectées ?	Section III, utilisateurs et objectifs Section VI(a), éléments de données
Quel est l'objectif de cette collecte de données ?	Annexe D, objectifs et besoins de données
Qui est le responsable de collecter les données ?	Section V, améliorer la qualité des données Annexe I, schémas opérationnels du RDS
Où est-ce que les données sont stockées et pendant combien de temps ?	Section VIII, modèles de RDS possibles Section VIII(d), stockage des données
Où est-ce que les données sont déposées et pendant combien de temps ?	Section VIII(d), principes relatifs au stockage, au dépôt fiduciaire et à l'inscription
Qui a besoin des données et pourquoi ?	Section III, utilisateurs et objectifs
Qui a besoin d'accéder aux registres d'accès aux données et pourquoi ?	Section VI(d), principes relatifs à la responsabilité et à l'audit
Accès public à des détails relatifs à l'enregistrement du nom de domaine ?	Section IV(b), accès non authentifié et sécurisé aux données Section VI(a), éléments de données Section VII, améliorer la vie privée du titulaire du ND
Accès des représentants de la loi à des détails relatifs à l'enregistrement d'un nom de domaine ?	Section III, utilisateurs et objectifs Section VI(b), principes pour l'accès aux données de la part des représentants de la loi
Accès des titulaires de droits de propriété	Section III, utilisateurs et objectifs

Questions et orientations du Conseil	Sections du rapport
intellectuelle à des détails relatifs à l'enregistrement d'un nom de domaine ?	
Accès des agents de sécurité à des détails relatifs à l'enregistrement d'un nom de domaine ?	Section III, utilisateurs et objectifs
Quelle valeur le public réalise-t-il de par l'accès aux données d'enregistrement ?	Section II(b), objectif Section III, utilisateurs et objectifs
De toutes les données d'enregistrement disponibles, à quelles données le public a-t-il besoin d'avoir accès ?	Section VI(a), éléments de données
Le protocole WHOIS est-il le meilleur choix pour fournir cet accès ?	Section IV(b), accès non authentifié et sécurisé aux données Annexe G, capacité des protocoles EPP et RDAP à soutenir le RDS
Sécurité	
Que comprend le besoin légitime des représentants de la loi ?	Section III, utilisateurs et objectifs Section VI(b), principes pour l'accès aux données de la part des représentants de la loi
Comment un représentant de la loi est-il identifié ?	Section IV(c), principes d'accréditation d'utilisateur du RDS Section VI(b), principes pour l'accès aux données de la part des représentants de la loi
Quelles données d'enregistrement comprennent l'identité réelle de la partie responsable et jusqu'à quel niveau d'exactitude ?	Section V, améliorer la qualité des données Section VI(a), éléments de données Section VII(b), identifiants protégés sécurisés
Quelles données d'enregistrement comprennent des informations précieuses pour les représentants de la loi qui cherchent l'identité réelle de la partie responsable et jusqu'à quel niveau d'exactitude ?	Section III, utilisateurs et objectifs Annexe D, objectifs et besoins de données
Le protocole WHOIS est-il le meilleur choix pour fournir ceci ?	Section IV(b), accès non authentifié et sécurisé aux données Annexe G, capacité des protocoles EPP et RDAP à soutenir le RDS
Titulaires de droits de propriété intellectuelle	
L'accès aux données d'enregistrement du nom de domaine souhaité est-il cohérent avec l'accès que les titulaires de droits de propriété	Section III, utilisateurs et objectifs Section IV(c), principes d'accréditation d'utilisateur du RDS

Questions et orientations du Conseil	Sections du rapport
intellectuelle ont à des types de données similaires dans d'autres secteurs ?	
Comment un titulaire de droits de propriété intellectuelle est-il identifié ?	Section IV(c), principes d'accréditation d'utilisateur du RDS
De toutes les données d'enregistrement disponibles, à quelles données le titulaire de droits de propriété intellectuelle a-t-il besoin d'avoir accès ?	Section III, utilisateurs et objectifs Annexe D, objectifs et besoins de données
Quelles données d'enregistrement est-il approprié de rendre disponibles ?	Section VI(a), éléments de données
Le protocole WHOIS est-il la méthode appropriée pour l'accès ?	Section IV(b), accès non authentifié et sécurisé aux données Annexe G, capacité des protocoles EPP et RDAP à soutenir le RDS

ANNEXE B : ÉTUDES EVALUANT LES INSUFFISANCES DU WHOIS

- Rapport SSAC - SAC 051
- Rapport SSAC - SAC 054
- Rapport SSAC - SAC 055
- Principes WHOIS du GAC
- Rapport final de l'équipe de révision des politiques du WHOIS
- Projet de procédure de l'ICANN pour gérer les conflits entre le WHOIS et les lois en matière de vie privée
- Inventaire des exigences de service WHOIS - rapport final
- Rapport initial de l'équipe de travail spécifique sur le WHOIS 2 (2009)
- Rapport final de l'équipe de travail spécifique sur les services du WHOIS (2007)
- Étude pour évaluer les solutions relatives à la soumission et à l'affichage des données de contact internationalisées
- Rapport final sur le WHOIS épais de la GNSO
- Rapport intérimaire de l'EWG sur les données d'enregistrement internationalisées
- Révision de la procédure de l'ICANN pour gérer les conflits entre le WHOIS et les lois en matière de vie privée
- Études sur le WHOIS de la GNSO y compris
    - Étude sur l'exactitude des informations de contact des titulaires de ND dans le WHOIS
    - Étude sur la prévalence des noms de domaine enregistrés utilisant un service d'anonymisation ou d'intermédiation parmi les 5 top gTLD
    - Étude relative au mauvais usage du WHOIS
    - Étude d'identification du titulaire de nom de domaine du WHOIS
    - l'étude concernant l'abus du service d'anonymisation et d'intermédiation du WHOIS
    - Enquête de faisabilité du relais et de la divulgation d'anonymisation/d'intermédiation du WHOIS + annexes

ANNEXE C : EXEMPLES DE CAS D'UTILISATION

Tel que décrit dans la section III, l'EWG a analysé des cas d'utilisation réels impliquant le système actuel du WHOIS pour identifier des utilisateurs qui souhaitent un accès à des données d'enregistrement de gTLD, leurs objectifs ce faisant et les parties prenantes et données concernées. Une liste des cas d'utilisation représentatifs considérés par l'EWG est fournie ci-dessous.

Objectif	Exemples de cas d'utilisation
Contrôle du nom de domaine	Création d'un compte d'enregistrement de nom de domaine
	Surveillance de la modification de données de noms de domaine
	Gestion du portefeuille des noms de domaine
	Démarrage de transfert de nom de domaine
	Suppressions des noms de domaine
	Actualisations DNS du nom de domaine
	Renouvellement de noms de domaine
	Validation du contact du nom de domaine
Protection des données personnelles	Contact fournisseur de services d'intermédiation / d'anonymisation
	Contact approbateur d'identifiant sécurisé
Résolution des problèmes techniques	Contact avec le personnel technique des noms de domaine
Certification des noms de domaine	Émission de certification des noms de domaine
Utilisation individuelle d'Internet	Contact avec le monde réel
	Protection du consommateur
Achat ou vente des noms de domaine commerciaux	Vente de noms de domaine par un intermédiaire
	Analyse des risques d'un nom de domaine (*Trademark Clearance*)
	Acquisition de noms de domaine
	Demande d'achat d'un nom de domaine
	Historique d'enregistrement d'un nom de domaine
	Noms de domaine pour des titulaires de nom de domaine spécifiques
Recherche académique/d'intérêt public du nom de domaine	Historique d'enregistrement d'un nom de domaine
	Noms de domaine pour des contacts spécifiques
	Enquête sur les titulaires de noms de domaine ou contacts désignés
Actions en justice	Contact de l'utilisateur d'un nom de domaine

Objectif	Exemples de cas d'utilisation
	Combattre l'utilisation frauduleuse des données d'enregistrement
	Historique de titulaire d'un nom de domaine
	Noms de domaine pour des contacts spécifiques
Exécution des contrats/règlementation	Enquête fiscale en ligne
	Procédures UDRP
	Conformité contractuelle de l'écosystème du RDS
Enquête policière & réduction des abus de DNS	Examiner les noms de domaine abusifs
	Enquêter sur l'activité criminelle hors ligne
	Services de réputation en matière de noms de domaine
	Enquêter sur l'activité criminelle en ligne
	Point de contact pour les abus des noms de domaine compromis
Transparence du DNS	Accès aux données d'enregistrement publiques
Activités malveillantes sur Internet	Piratage du nom de domaine
	Enregistrement malveillant d'un nom de domaine
	Fouille des données d'enregistrement pour Pourriel/Escroquerie

Tableau 7. Exemples de cas d'utilisation

Pour illustrer la méthodologie de l'EWG, un seul cas d'utilisation est présenté ci-dessous. Se référer à la section III pour des descriptions supplémentaires de chaque cas d'utilisation et des utilisateurs du RDS et besoins de données connexes.

Résolution de question technique - contact avec le personnel technique du nom de domaine

But/Scénario #1 :

Une personne a un problème opérationnel ou technique avec un nom de domaine enregistré. Elle veut savoir s'il existe quelqu'un qu'elle puisse contacter pour résoudre le problème en temps réel ou quasi réel. Elle utilise donc le RDS pour identifier la personne appropriée, le rôle ou l'entité qui a la capacité de résoudre le problème. Une liste incomplète d'exemples de questions techniques inclut des problèmes d'envoi et de réception de courriel, des problèmes de résolution du DNS et des problèmes fonctionnels relatifs à un site Web.

Format bref de cas d'utilisation

Cas d'utilisation : Identifier la personne, le rôle ou l'entité qui peut aider à résoudre un problème technique concernant un nom de domaine.

Cas d'utilisation principal : Une personne accède au RDS pour obtenir des informations de contact associées à des noms de domaine enregistrés sous un TLD ou des TLD. La personne soumet un nom de domaine au RDS pour le traitement. Le RDS retourne l'information associée au nom de domaine qui identifie la personne, le rôle ou l'entité qui peut être contactée pour résoudre les problèmes techniques.

Format occasionnel de cas d'utilisation

Titre : Identifier la personne, le rôle ou l'entité qui peut résoudre un problème technique concernant un nom de domaine.

Acteur principal : Une personne qui a un problème technique avec un nom de domaine enregistré.

Autres parties prenantes : Opérateur du RDS ; personne, rôle ou entité associés au nom de domaine enregistré qui peut résoudre des problèmes techniques ; titulaire de nom de domaine (qui peut vouloir être au courant des questions opérationnelles) ; validateur (qui peut avoir émis un ID de contact au contact technique) ; bureau d'enregistrement ou fournisseur d'hébergement (qui peut fournir un service opérationnel) ; fournisseur de services d'anonymisation/d'intermédiation accrédité (qui peut aider à joindre la personne, le rôle ou l'entité associés au nom de domaine qui peut résoudre des questions techniques).

Objet : Interaction avec le RDS

Niveau : Tâche utilisateur

Éléments de données : Les éléments de données qui permettent une communication en temps réel ou quasi réel sont les plus utiles dans le contexte de ce cas d'utilisation. Ceux-ci incluent une adresse email, une adresse de messagerie instantanée, un numéro de téléphone et/ou un indicateur qui identifie la méthode de contact préférée indiquée par le titulaire du nom de domaine. La section 4 du RFC 2142 décrit des recommandations relatives aux adresses email abus@, noc@, sécurité@ afin de « fournir un recours aux clients, fournisseurs et autres qui ont des difficultés avec le service Internet de l'organisation », mais il est important de noter que la nature publique de ces adresses les rend souvent attirantes pour les expéditeurs de courriels en masse non sollicités (pourriels).

Historique : Une personne (un requérant) confrontée à une question technique liée à un nom de domaine enregistré accède au RDS afin d'obtenir des informations relatives à des noms de domaine enregistrés sous un TLD ou des TLD. Le RDS pourrait être accessible via un site Web ou d'autres moyens de traitement électronique.

Le requérant soumet un nom de domaine au système pour le traitement.

Le RDS traite la demande et soit signale des conditions d'erreur soit procède à une requête des données d'enregistrement gTLD afin d'obtenir les informations associées à cette personne, ce rôle ou cette entité précédemment identifiés comme ressources pouvant aider à résoudre les questions techniques relatives à ce nom de domaine.

Le RDS renvoie les données d'enregistrement associées au nom de domaine ou une condition d'erreur rencontrée lors de la récupération des données.

Figure 9. Exemple de cas d'utilisation

ANNEXE D : OBJECTIFS ET BESOINS DE DONNÉES

L'EWG a analysé des cas d'utilisation pour identifier des utilisateurs qui souhaitent un accès à des données d'enregistrement de gTLD, leurs objectifs ce faisant et les parties prenantes et données concernées. Le tableau suivant récapitule les éléments de données du RDS recommandés dans la section IV et attribués à des objectifs admissibles définis dans la Section III. Se référer à la section IV pour les recommandations de collecte et de divulgation pour chaque élément de données.

Élément de données	Objectifs
Nom de domaine	Tous
Serveurs DNS	Contrôle du nom de domaine Résolution des problèmes techniques Certification des noms de domaine Achat ou vente des noms de domaine commerciaux Recherche du DNS académique/d'intérêt public Exécution des contrats/règlementation Enquête policière & réduction des abus de DNS
Nom du titulaire du nom de domaine et/ou organisation Type de titulaire de nom de domaine ID de contact du titulaire du nom de domaine Statut de validation du contact du titulaire du nom de domaine Horodatage dernière validation du contact du titulaire du nom de domaine	Tous
Identifiant de l'entreprise du titulaire du nom de domaine :	Contrôle du nom de domaine Certification des noms de domaine Utilisation individuelle d'Internet Achat ou vente des noms de domaine commerciaux Actions en justice Recherche du DNS académique/d'intérêt public Exécution des contrats/règlementation Enquête policière & réduction des abus de DNS Transparence du DNS
Adresse postale du titulaire du nom de domaine, y compris : Adresse de résidence du titulaire du nom de domaine Ville du titulaire du nom de domaine État / province du titulaire du nom de domaine Code postal du titulaire du nom de domaine Pays du titulaire du nom de domaine	Contrôle du nom de domaine Certification des noms de domaine Achat ou vente des noms de domaine commerciaux * Recherche du DNS académique/d'intérêt public * Actions en justice* Exécution des contrats/règlementation Enquête policière & réduction des abus de DNS

Élément de données	Objectifs
Numéro de poste téléphonique du titulaire du nom de domaine Numéro de poste téléphonique alternatif du titulaire du nom de domaine	Contrôle du nom de domaine Résolution des problèmes techniques Certification des noms de domaine Achat ou vente des noms de domaine commerciaux * Recherche du DNS académique/d'intérêt public * Actions en justice* Exécution des contrats/règlementation Enquête policière & réduction des abus de DNS
Adresse électronique du titulaire du nom de domaine Adresse électronique alternative du titulaire du nom de domaine	Tous
Numéro de poste de télécopie du titulaire du nom de domaine	Contrôle du nom de domaine Certification des noms de domaine Achat ou vente des noms de domaine commerciaux * Recherche du DNS académique/d'intérêt public * Actions en justice* Exécution des contrats/règlementation
Nouvelles méthodes de contact que les titulaires de noms de domaine peuvent choisir de publier : Message texte du titulaire de nom de domaine Messagerie instantanée du titulaire de nom de domaine Médias sociaux du titulaire de nom de domaine Médias sociaux alternatifs du titulaire de nom de domaine ID de contact du titulaire du nom de domaine URL en cas d'abus du titulaire du nom de domaine	Pourrait être utile pour chaque objectif admissible en tant qu'alternative à l'adresse email du titulaire du nom de domaine
ID du contact administratif Éléments de données du contact administratif	Contrôle du nom de domaine Certification des noms de domaine Achat ou vente des noms de domaine commerciaux Recherche du DNS académique/d'intérêt public Transparence du DNS
ID du contact juridique Éléments de données du contact juridique	Contrôle du nom de domaine Certification des noms de domaine Recherche du DNS académique/d'intérêt public Actions en justice Exécution des contrats/règlementation Transparence du DNS
ID du contact technique Éléments de données du contact technique	Contrôle du nom de domaine Résolution des problèmes techniques Certification des noms de domaine Recherche du DNS académique/d'intérêt public Transparence du DNS

Élément de données	Objectifs
ID du contact en cas d'abus Éléments de données de contact en cas d'abus	Contrôle du nom de domaine Certification des noms de domaine Recherche du DNS académique/d'intérêt public Enquête policière/réduction des abus de DNS Transparence du DNS
ID contact fournisseur PP Éléments de données de contact fournisseur PP	Contrôle du nom de domaine Protection des données personnelles Certification des noms de domaine Recherche du DNS académique/d'intérêt public Transparence du DNS
ID du contact commercial Éléments de données du contact commercial	Contrôle du nom de domaine Certification des noms de domaine Utilisation individuelle d'Internet Recherche du DNS académique/d'intérêt public Transparence du DNS
Délégation DNSSEC	Contrôle du nom de domaine Recherche du DNS académique/d'intérêt public
Statut de l'enregistrement Statut du client (bureau d'enregistrement) Statut du serveur (registre)	Contrôle du nom de domaine Achat ou vente des noms de domaine commerciaux Recherche du DNS académique/d'intérêt public Exécution des contrats/règlementation Enquête policière/réduction des abus de DNS
Bureau d'enregistrement Revendeur URL du bureau d'enregistrement Numéro IANA du bureau d'enregistrement Adresse électronique de contact avec le bureau d'enregistrement en cas d'abus Numéro de téléphone de contact avec le bureau d'enregistrement en cas d'abus URL du site de plaintes Internic	Contrôle du nom de domaine Achat ou vente des noms de domaine commerciaux Recherche du DNS académique/d'intérêt public Exécution des contrats/règlementation Enquête policière/réduction des abus de DNS Transparence du DNS
Juridiction du bureau d'enregistrement Juridiction du registre Langue de l'accord d'enregistrement	Tous
Date de l'enregistrement initial	Contrôle du nom de domaine Achat ou vente des noms de domaine commerciaux Recherche du DNS académique/d'intérêt public Exécution des contrats/règlementation
Date de création Date de mise à jour Date d'expiration du bureau d'enregistrement	Contrôle du nom de domaine Achat ou vente des noms de domaine commerciaux Recherche du DNS académique/d'intérêt public Exécution des contrats/règlementation Enquête policière/réduction des abus de DNS

Note : L'accès à des éléments de données de titulaire de nom de domaine sécurisés quelquefois nécessaire pour des objectifs marqués * ci-dessus peut inclure une approbation de besoin de savoir ; voir section III pour la description de « données sécurisées approuvées ».

ANNEXE E : ILLUSTRATIONS D'ACCÈS SÉCURISÉ ET NON AUTHENTIFIÉ

Le registre de données d'enregistrement suivant proroge l'exemple WHOIS du RAA 2013 pour refléter les principes RDS recommandés pour la collecte et la divulgation de données.

Il est facultatif de collecter les éléments en gris ; les autres sont obligatoires.
Les éléments en gras sont toujours publics ; le reste peut être sécurisé, au choix du titulaire du nom de domaine ou du détenteur du contact.

Statut de l'enregistrement : x **Délégation DNSSEC : signedDelegation** **Statut du client : SupressionInterdite, RenouvellementInterdit, TransfertInterdit** **Statut du serveur : SupressionInterdite, RenouvellementInterdit, TransfertInterdit** **Bureau d'enregistrement : BUREAU D'ENREGISTREMENT EXEMPLE SARL** **Revendeur : REVENDEUR EXEMPLE** **Juridiction du bureau d'enregistrement : JURIDICTION EXEMPLE** **Juridiction du registre : JURIDICTION EXEMPLE** **Langue de l'accord d'enregistrement : ANGLAIS** **Date de création : 2000-10-08T00:45:00Z** **Date de l'enregistrement initial : 2000-10-08T00:45:00Z** **Date d'expiration de l'enregistrement du bureau d'enregistrement : 2010-10-08T00:44:59Z** **Date de mise à jour : 2009-05-29T20:13:00Z** **URL du bureau d'enregistrement : http://www.example-registrar.tld** **Numéro IANA du bureau d'enregistrement : 5555555** **Adresse électronique de contact avec le bureau d'enregistrement en cas d'abus : email@registrar.tld** **Numéro de téléphone de contact avec le bureau d'enregistrement en cas d'abus : email@registrar.tld +1,1235551234** **URL du site de plaintes Internic : http://wdprs.internic.net/**	Fourni par le registre ou le bureau d'enregistrement
Nom de domaine : EXEMPLE.TLD **Serveur de nom : NS01.EXAMPLE-BUREAU D'ENREGISTREMENT.TLD** Nom du titulaire du nom de domaine : TITULAIRE DU ND EXEMPLE **Type de titulaire de nom de domaine : PERSONNE MORALE** **ID de contact du titulaire du ND : xxxx-xxxx** (émis par le validateur accrédité RDS) **Statut de validation du contact du titulaire du ND (par le validateur)**	collecté du titulaire du nom de domaine

Horodatage dernière validation du contact du titulaire du ND (par le validateur) Organisation du titulaire du nom de domaine : ORGANISATION EXEMPLE Identifiant de l'entreprise du titulaire du nom de domaine : D-U-N-S #12345 (émis par Dunn and Bradstreet) **Adresse électronique du titulaire du nom de domaine : EMAIL@EXEMPLE.TLD** Adresse électronique alternative du titulaire du nom de domaine : EXEMPLE@OTHERDN.TLD Rue du titulaire du nom de domaine : 123, RUE EXEMPLE Ville du titulaire du nom de domaine : VILLE EXEMPLE État / province du titulaire du nom de domaine : AP Code postal du titulaire du nom de domaine : A1A1A1 **Pays du titulaire du nom de domaine** : AA Numéro de téléphone du titulaire du nom de domaine : +1,5555551212 Numéro de poste du titulaire du nom de domaine : 1234 Numéro de téléphone alternatif du titulaire du nom de domaine : <cellulaire> Numéro de poste téléphonique alternatif du titulaire du nom de domaine 1234 Numéro de télécopie du titulaire de nom de domaine : +1,5555551213 Numéro de poste de télécopie du titulaire du nom de domaine : 4321 Message texte du titulaire de nom de domaine : <numérotexto> Messagerie instantanée du titulaire de nom de domaine : <IMhandle> Médias sociaux du titulaire de nom de domaine : <SMhandle> Médias sociaux alternatifs du titulaire de nom de domaine : <AutreSMhandle> URL de contact du titulaire du nom de domaine : <lien à formulaire me contacter ou instructions> URL de contact du titulaire du nom de domaine : <lien à formulaire de signalement d'abus ou instructions>	
ID contact administrateur : xxxx-xxxx **(suivi par coordonnées de contact PBC Admin ***)	Le titulaire du ND doit publier les contacts basés sur objectifs
ID contact technique : xxxx-xxxx **(suivi par coordonnées de contact PBC Tech ***)	
ID contact juridique : xxxx-xxxx **(suivi par coordonnées de contact PBC juridique ***)	
ID contact en cas d'abus : xxxx-xxxx **(suivi par coordonnées de contact PBC en cas d'abus ***)	

ID contact commercial: xxxx-xxxx (seulement si type de titulaire de ND = personne morale) (suivi par coordonnées de contact PBC commercial*)	
ID contact P/P : xxxx-xxxx (seulement si type de titulaire de ND = fournisseur P/P) (suivi par coordonnées de contact PBC fournisseur P/P*)	

Clé : Les éléments en gris sont collectés à titre facultatif/conditionnel ; les autres sont obligatoires.

Les éléments en gras sont toujours publics ; le reste peut être sécurisé, au choix du titulaire du nom de domaine ou du détenteur du contact. * Les éléments de données des PBC ne sont entièrement illustrés ici.

Exemple #1 : Demande publique non authentifiée pour des objectifs de résolution de questions techniques

1) L'utilisateur soumet une demande non authentifiée au RDS
(ND = MerchantZ.gtld, objectif = résolution de question technique, données = toutes)

2) Le RDS évalue la demande :
Pas d'authentification, parce que la demande est non authentifiée
Pas d'autorisation, l'accès à des données publiques est octroyé
L'accès est limité aux données publiques nécessaires pour la résolution de la question technique --
c'est-à-dire toutes les données publiques relatives au nom de domaine PLUS les données de contact technique

3) Le RDS extrait les éléments de données requis :
Les données du MerchantZ.gtld sont extraites du cache du RDS (synchronisé) ou du registre (fédéré) fournissant uniquement les éléments de données publics définis pour cet objectif, y compris

ID contact titulaire du ND = 12345
Type de titulaire du ND = personne morale
Organisation du titulaire du ND = MerchantZ, Inc.[38]
ID contact technique = 67890

L'ID du contact technique [67890] est extrait du cache du RDS ou du validateur, obtenant ainsi seulement les éléments de données publics publiés explicitement par ce contact pour cet objectif, y compris

ID PBC = 67890

Nom du PBC = <nom de l'entité chargée de résoudre les questions techniques pour le nom de domaine *MerchantZ.gtld*>

Adresse email du PBC = <adresse email obligatoire de l'entité chargée de résoudre les questions techniques pour le nom de domaine *MerchantZ.gtld*>

Adresse email alternative du PBC = <adresse email alternative recommandée de l'entité chargée de résoudre les questions techniques pour le nom de domaine *MerchantZ.gtld*>

[38] L'organisation du titulaire du nom de domaine est collectée des titulaires de noms de domaine qui indiquent comme type de titulaire de nom de domaine personne morale ou fournisseur de services PP accrédité ; peut être absente lorsque le type de titulaire de nom de domaine est non déclaré

Numéro de téléphone du PBC = <numéro de téléphone recommandé de l'entité chargée de résoudre les questions techniques pour le nom de domaine *MerchantZ.gtld*>

URL de contact du PBC = <lien de contact recommandé publié par l'entité chargée de résoudre les questions techniques pour le nom de domaine *MerchantZ.gtld*>

<tous éléments de données publics publiés par cette entité>

4) Le RDS renvoie une condition d'erreur ou une réponse réussie à l'utilisateur. Par exemple :

Nom de domaine : MerchantZ.gtld *Statut d'enregistrement : x* *Statut du client : Suppressioninterdite, renouvellementinterdit, transfertinterdit* *Statut du serveur : SupressionInterdite, RenouvellementInterdit, TransfertInterdit* *Bureau d'enregistrement BUREAU D'ENREGISTREMENT EXEMPLE SARL* *Juridiction du bureau d'enregistrement : JURIDICTION EXEMPLE* *Juridiction du registre : JURIDICTION EXEMPLE* *Langue de l'accord d'enregistrement : ANGLAIS* *Date de création : 2000-10-08T00:45:00Z* *Date d'expiration de l'enregistrement du bureau d'enregistrement : 2010-10-08T00:44:59Z* *Date de mise à jour: 2009-05-29T20:13:00Z* *URL du bureau d'enregistrement : http://www.bureauéd'enregistrement-exemple.tld* *Numéro IANA du bureau d'enregistrement : 5555555* *Email de contact en cas d'abus du bureau d'enregistrement : email@registrar.tld* *Téléphone de contact en cas d'abus du bureau d'enregistrement : +1.1235551234* *URL du site de plaintes Internic :http://wdprs.internic.net/*
Serveur de nom : NS01.BUREAU-D'ENREGISTREMENT-EXEMPLE.TLD *ID de contact du titulaire du ND = 12345* *Type de titulaire de ND = personne morale* *Organisation du titulaire du ND = MerchantZ, Inc.* *Email du titulaire du ND = 12345@MerchantZ.gtld* *Statut de validation du contact du titulaire du ND = validé du point de vue opérationnel* *Horodatage dernière validation du contact du titulaire du ND = x* *<Autres éléments de données facultatifs publics publiés par le titulaire du ND pour ce ND>*
ID du contact technique = 67890 *ID PBC = 67890* *Statut de validation du PBC = validé du point de vue opérationnel*

Horodatage dernière validation du PBC = x
Nom du PBC : TECHNICIEN EXEMPLE
Email PBC = 67890@SuperbHostingServices.gtld
Adresse électronique alternative du PBC = SuperbHostingServices@OtherDN.gtld
Numéro de téléphone du PBC =+1.1235567890
URL contact du PBC=TechSupport@SuperbHostingServices.gtld
<Éléments de données facultatifs publics publiés par ce PBC>

Exemple #2 : Demande sécurisée authentifiée pour des objectifs de résolution de questions techniques

1) L'utilisateur soumet une demande authentifiée au RDS
(ND = PersonY.gtld, objectif = résolution de question technique, données = toutes)

2) Le RDS évalue la demande :
   - Si « A » est authentique, la demande sécurisée est approuvée
   - Si « A » est un FSI accrédité, l'accès à la résolution de question technique est accordé
   - L'accès est limité aux données publiques+sécurisées requises pour la résolution de la question technique
   - L'accès est limité aux données publiques+sécurisées requises pour la résolution de la question technique --
     à savoir, toutes les données publiques+sécurisées demandées pour cet objectif PLUS contact technique

3) Le RDS extrait les éléments de données requis :
Les données du PersonY.gtld sont extraites du cache du RDS (synchronisé) ou du registre (fédéré) obtenant les éléments de données publics + sécurisés définis pour cet objectif, y compris :

ID contact titulaire du ND = 12345
Type de titulaire du ND = non déclaré
<tous éléments de données facultatifs publics ou sécurisés publiés par ce titulaire du ND – par exemple, si le titulaire du ND le choisit, son nom>
ID du contact technique = 67890[39]

L'ID du contact technique [67890] est extrait du cache du RDS ou du validateur, obtenant ainsi seulement les éléments de données publics et sécurisés publiés explicitement par ce contact pour cet objectif, y compris

ID PBC = 67890

Adresse email du PBC = <adresse email obligatoire de l'entité chargée de résoudre les questions techniques pour le nom de domaine *PersonY.gtld*>

[39] Si le titulaire du ND ne fournit pas d'ID de contact durant l'enregistrement du ND, il devrait être informé que ses propres adresses seront publiées comme PBC primaire et avoir la possibilité de consentir, de fournir un autre ID PBC primaire (par exemple, l'ID d'un fournisseur de services PP) ou annuler l'enregistrement.

Adresse email alternative du PBC = <adresse email alternative recommandée de l'entité chargée de résoudre les questions techniques pour ce ND>

Numéro de téléphone du PBC = <numéro de téléphone recommandé de l'entité chargée de résoudre les questions techniques pour ce ND>

URL de contact du PBC = <lien de contact recommandé publié par l'entité chargée de résoudre les questions techniques pour ce ND>

<tous éléments de données facultatifs publics ou sécurisés publiés par cette entité – par exemple, le numéro de messagerie texte SMS>

4) Le RDS renvoie une condition d'erreur ou une réponse réussie à l'utilisateur. Par exemple :

Nom de domaine : PersonY.gtld *Statut d'enregistrement : x* *Statut du client : Suppressioninterdite, renouvellementinterdit, transfertinterdit* *Statut du serveur : SupressionInterdite, RenouvellementInterdit, TransfertInterdit* *Bureau d'enregistrement BUREAU D'ENREGISTREMENT EXEMPLE SARL* *Juridiction du bureau d'enregistrement : JURIDICTION EXEMPLE* *Juridiction du registre : JURIDICTION EXEMPLE* *Langue de l'accord d'enregistrement : ANGLAIS* *Date de création : 2000-10-08T00:45:00Z* *Date d'expiration de l'enregistrement du bureau d'enregistrement : 2010-10-08T00:44:59Z* *Date de mise à jour: 2009-05-29T20:13:00Z* *URL du bureau d'enregistrement : http://www.example-registrar.tld* *Numéro IANA du bureau d'enregistrement : 5555555* *Email de contact en cas d'abus du bureau d'enregistrement : email@registrar.tld* *Téléphone de contact en cas d'abus du bureau d'enregistrement : +1.1235551234* *URL du site de plaintes Internic :http://wdprs.internic.net/*
Serveur de nom : NS01.BUREAU-D'ENREGISTREMENT-EXEMPLE.TLD *ID de contact du titulaire du ND = 12345* *Type de titulaire de ND = non déclaré* *Email du titulaire du ND = 12345@PersonY.gtld* *Statut de validation du contact du titulaire du ND = Validé du point de vue opérationnel* *Horodatage dernière validation du contact du titulaire du ND =x* *<Autres éléments de données facultatifs publics ou sécurisés publiés par le titulaire du ND pour le ND, comme le nom du titulaire du ND, son numéro SMS ou son URL de contact >*

ID du contact technique = 67890
ID PBC = 67890
Statut de validation du PBC = validé du point de vue opérationnel
Horodatage dernière validation du PBC = x
Nom du PBC : TECHNICIEN EXEMPLE
Email PBC = 67890@SuperbHostingServices.gtld
Adresse électronique alternative du PBC = SuperbHostingServices@OtherDN.gtld
Numéro de téléphone du PBC =+1.1235567890
URL contact du PBC=TechSupport@SuperbHostingServices.gtld
<Éléments de données facultatifs publics ou sécurisés publiés par ce PBC>

Exemple #3 : Demandes de données sécurisées approuvées pour des objectifs d'achat/de vente de nom de domaine ou d'action en justice

L'enquête sur une éventuelle violation de marque de commerce est illustrée ci-dessous, mais des points de départ et des étapes similaires s'appliquent à l'achat, la fusion/acquisition de nom de domaine et bien d'autres enquêtes dans le cadre de ces objectifs et d'autres objectifs.

Étape 1) L'utilisateur du RDS se connecte à une entité d'accréditation (définie à la section IV(c), Accréditation d'utilisateurs du RDS) et atteste que non seulement son objectif est une action en justice mais aussi que les données sont obtenues afin d'enquêter sur une violation éventuelle de marque de commerce de la part du sujet « X ». L'utilisateur fournit le nom et les coordonnées de contact de l'individu/de l'organisation objet d'intérêt. Les demandes au RDS pour cet objectif sont donc intrinsèquement limitées aux données d'enregistrement associées à ce sujet.

Étape 2) L'utilisateur du RDS peut alors procéder à une requête inverse sur les valeurs déjà connues à propos du sujet, recherchant dans le RDS une liste de noms de domaine qui inclut des valeurs données comme :

- Nom/organisation du titulaire du ND et/ou du PBC
- Téléphone/téléphone alternatif du titulaire du ND et/ou du PBC
- Adresses postales du titulaire du ND et/ou du PBC ou
- Adresse email/email alternatif du titulaire du ND et/ou du PBC

Certains de ces éléments de données peuvent être sécurisés. La requête inverse cherche ces éléments de données sécurisés approuvés mais uniquement pour la valeur donnée et l'objectif énoncé, tel que décrit dans l'attestation.

Étape 3) ayant obtenu une liste de noms de domaine sous enquête pour identifier ceux éventuellement impliqués dans la violation de marque de commerce faisant l'objet de l'enquête, l'utilisateur du RDS peut alors effectuer des demandes concernant ces domaines pour obtenir les données nécessaires à l'évaluation des cas, notamment :

- ID du contact
- Dates d'enregistrement
- Juridiction du bureau d'enregistrement
- Juridiction du registre
- Pays du titulaire du ND (juridiction du titulaire du ND)
- Organisation du titulaire du ND et
- Identifiant de l'entreprise du titulaire du ND

Ces mêmes informations peuvent aussi être demandées dans des requêtes WhoWas concernant ces noms de domaine. Dans cette étape, tous les éléments de données sont publics, sauf le pays du titulaire du ND qui est sécurisé.

Étape 4) ayant conclu qu'une action suivante est appropriée, l'utilisateur du RDS peut procéder à une demande au RDS afin d'extraire l'ID du contact juridique public publié et autres données de contact connexes (y compris le nom et l'organisation du PBC, son numéro de téléphone et son adresse postale). Ces résultats peuvent être utilisés pour essayer de contacter le contact juridique désigné par le titulaire du ND, ou pour intenter une action en justice, déposer une plainte UDRP ou prendre d'autres mesures judiciaires.

Étape 5) si le contact juridique renie la responsabilité pour le nom de domaine, les coordonnées complètes de contact du titulaire du ND peuvent être nécessaires pour intenter une action en justice. Une grande partie de ces données peuvent être déjà connues dans l'étape 1, et non obtenues du RDS. Toutefois, certaines lacunes peuvent exister auxquelles il faut parer à ce point.

Cet exemple illustre les interactions avec le RDS dans le cadre d'enquêtes et d'éventuelles actions en justice ayant trait à une violation de marque de commerce. Cependant, une série d'étapes très similaire peut avoir lieu pour d'autres actions en justice et lors d'enquêtes sur les actifs du nom de domaine en cas d'achat/de vente. Dans les cas impliquant des données sécurisées approuvées, l'accréditeur devrait être responsable du contrôle de l'accès pour identifier les requêtes qui dépassent éventuellement le champ étroit confirmé et pour prendre des mesures afin d'éviter l'abus et d'appliquer les conditions générales. Le fait que l'attestation de l'utilisateur du

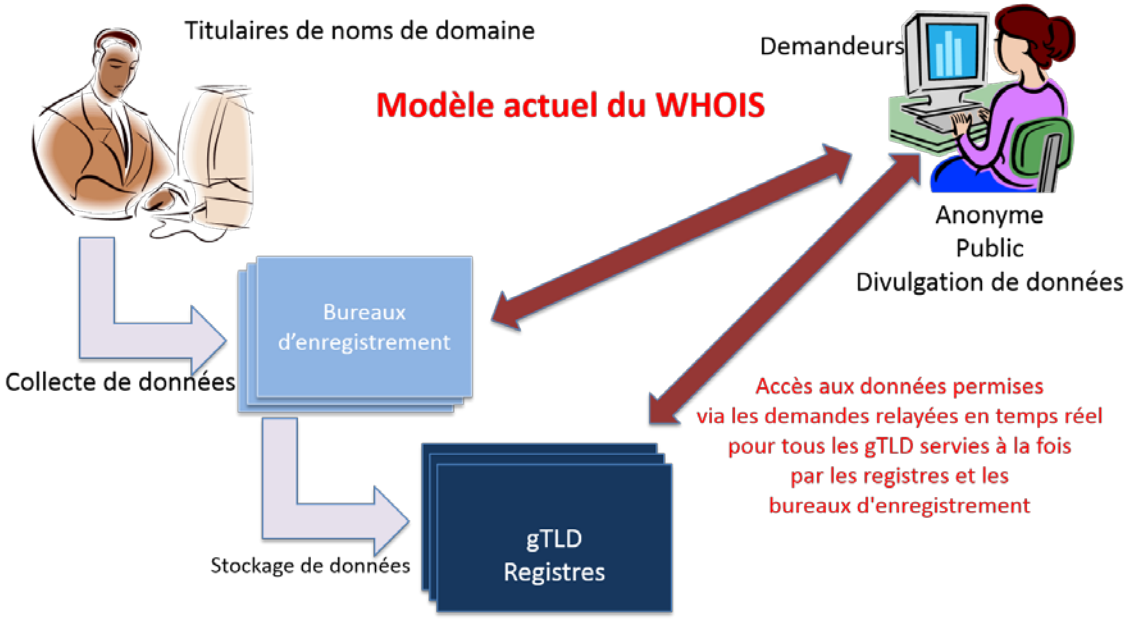
RDS figure dans le dossier aidera l'accréditeur à contrôler l'accès et à détecter un éventuel abus. Ceci s'avèrera également dissuasif pour les enquêtes à l'aveuglette.

ANNEXE F : MODÈLES DE SYSTÈMES CONSIDÉRÉS ET MÉTHODOLOGIE

En plus des modèles précédemment décrits dans les modèles de RDS possibles, l'EWG a considéré les alternatives suivantes mais les a trouvées moins viables que les modèles fédéré ou synchronisé, pour les raisons résumées ci-dessous.

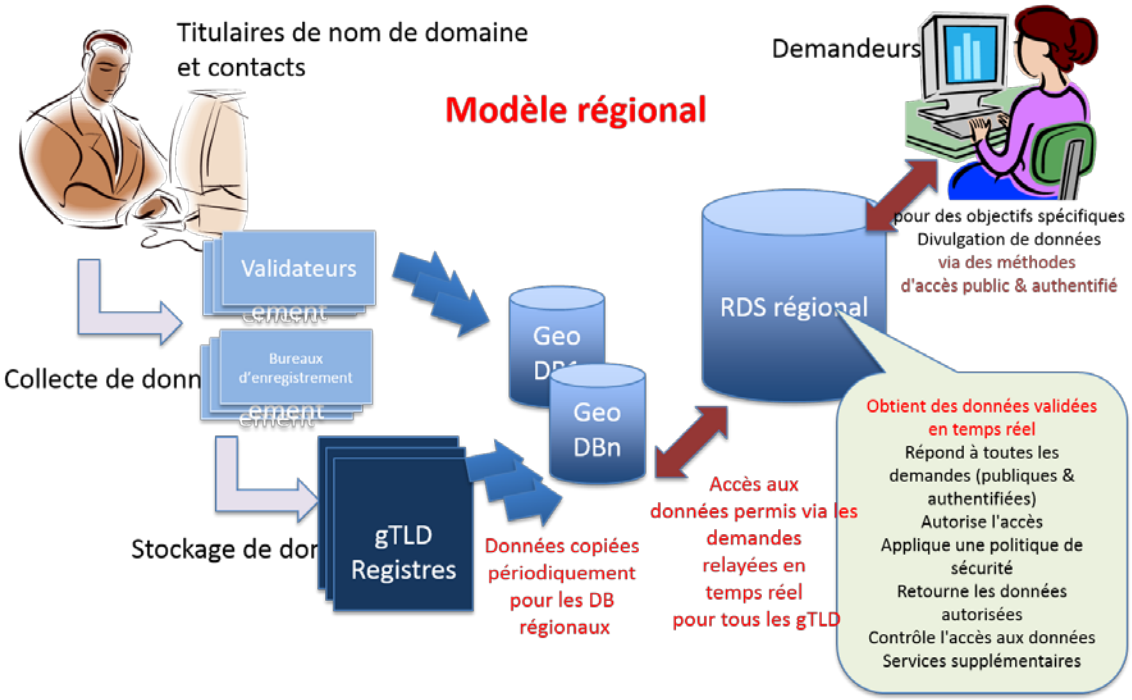
WHOIS actuel

Ce modèle décrit l'approche autonome entièrement distribuée utilisée par le système WHOIS actuel, où chaque registre et bureau d'enregistrement offre ses propres services WHOIS sans intégration à travers tous les gTLD. Bien qu'un portail centralisé pour permettre l'accès au WHOIS à travers tous les gTLD puisse être bâti, chaque registre fournirait quand même son propre stockage séparément géré et son propre accès, soit directement (épais) soit via une délégation aux bureaux d'enregistrement (mince).



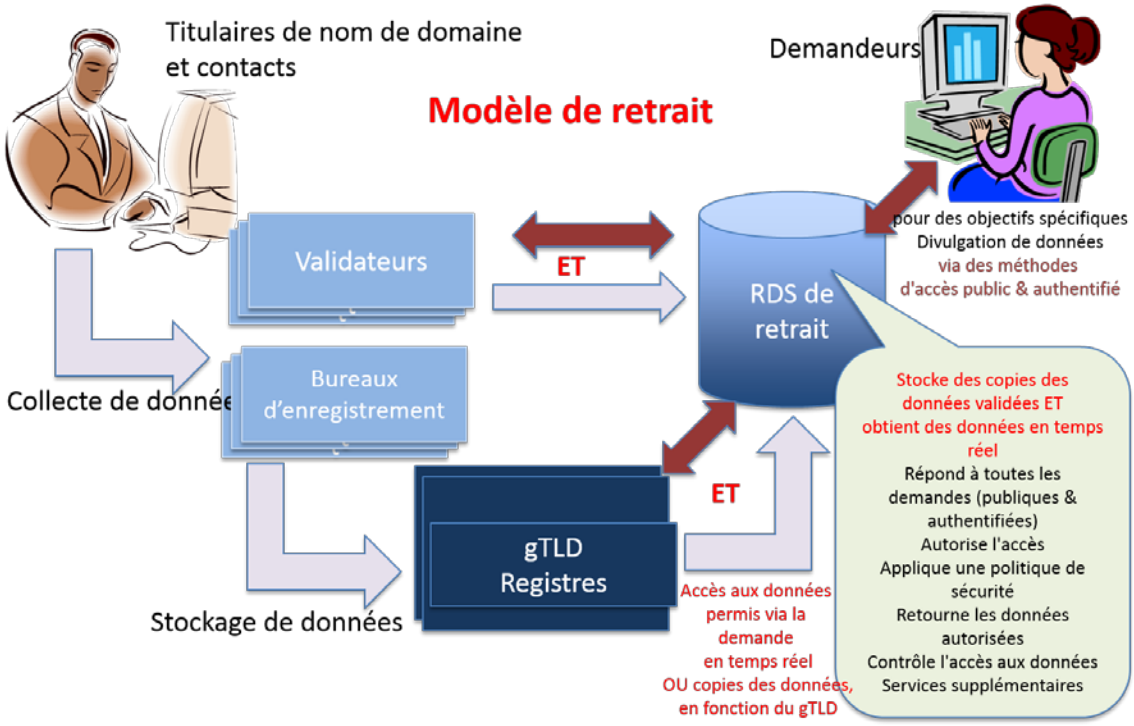
Modèle régional

Ce modèle décrit un RDS qui copie régulièrement les données à partir de zone de stockage distribuées gérées par les registres et les validateurs dans des zones de stockage régional situées de par le monde. Les registres et les validateurs continuent à stocker des données, mais les copies régionales de ces données peuvent être utilisées par le RDS pour traiter les demandes d'accès de manière plus efficace. Les accès au stockage régional sont gérés par le RDS mais sont régis par les lois de la juridiction dans laquelle chaque stockage régional est situé.



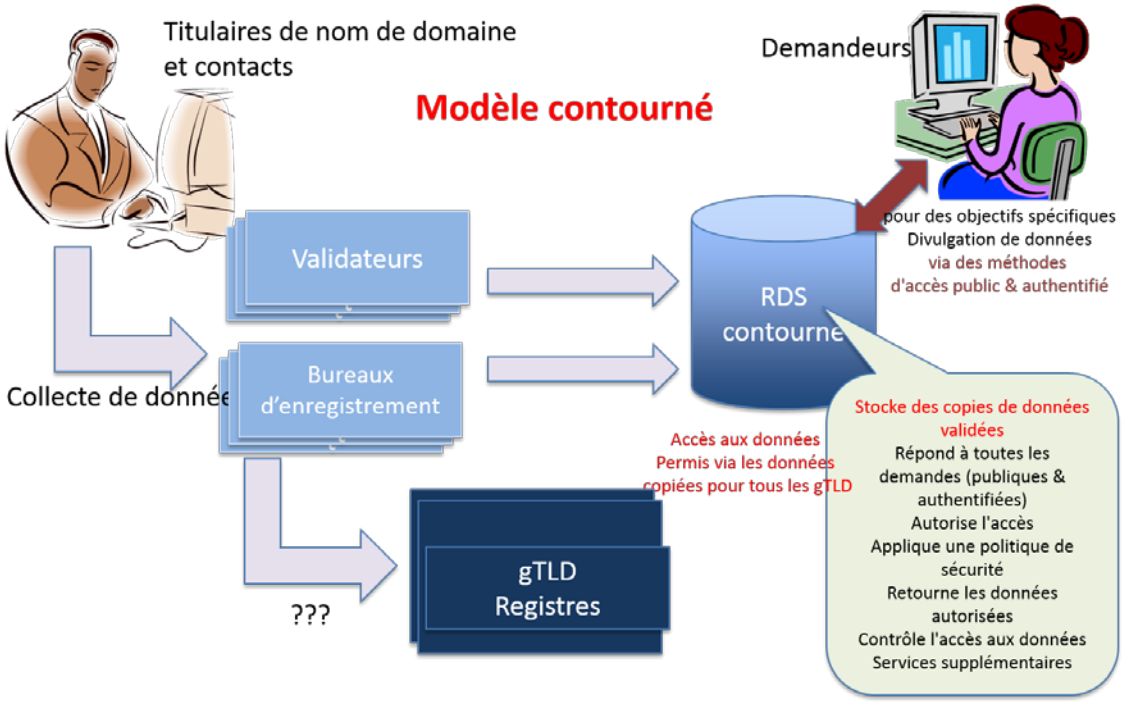
Modèle de retrait

Ce modèle décrit un RDS qui copie régulièrement les données à partir de zone de stockage distribuées gérées par les registres dans un stockage synchronisé géré par le RDS. Selon ce modèle, tout registre peut choisir de se retirer du stockage synchronisé dans la mesure où il convient de fournir l'infrastructure nécessaire pour traiter les demandes importantes tel que requis dans les accords de niveau de service de performance et de disponibilité (SLA).



Modèle contourné

Ce modèle décrit un RDS qui copie régulièrement les données à partir de zone de stockage distribuées gérées par les bureaux d'enregistrement dans un stockage synchronisé géré par le RDS. Selon ce modèle, les registres sont contournés en tant que source d'informations d'enregistrement ; au lieu de cela, le RDS dessert les demandes en utilisation des données d'enregistrement synchronisées copiées directement des sources faisant autorité.



Méthodologie appliquée pour comparer les modèles de systèmes

L'EWG a considéré les coûts connexes et les vulnérabilités en matière de sécurité inhérents au système du WHOIS actuel, dont un grand nombre est traité dans les rapports énumérés à l'annexe B où les insuffisances du WHOIS sont documentées. Les coûts et les vulnérabilités du système du WHOIS actuel ont été comparés et mis en contraste avec les modèles possibles. En outre, l'EWG a comparé les avantages et les inconvénients en matière de sécurité de chacun des modèles possibles par rapport aux critères suivants :

Incidences sur la sécurité

- **Point unique de défaillance :** Prenant en compte l'utilisation d'une architecture distribué et un fournisseur de services primaire, dans quelle mesure le modèle est-il vulnérable en cas de défaillance d'un système unique ? La défaillance d'un système empêcherait-elle provisoirement l'accès à toutes ou à uniquement certaines informations d'enregistrement ? **Note :** Une conception de base de données et des pratiques d'exploitation robustes devraient être utilisées pour fournir une redondance et une sauvegarde de données internes. Il s'agit donc en fait de la disponibilité de données durant la défaillance.
- **En cas d'abus interne :** Dans quelle mesure le modèle est-il vulnérable à l'abus d'initié dans l'accès administratif/d'opérateur aux informations d'enregistrement stockées par ou passant à travers tout système qui compose le modèle ? Un abus d'initié résulterait-il en un accès non autorisé à toutes ou à certaines données ? Dans quelle mesure serait-il facile d'appliquer des contrôles pour détecter/dissuader les abus d'initiés ?
- **En cas d'abus externe :** Dans quelle mesure le modèle est-il vulnérable à une attaque externe contre tout système composant le modèle ? Une attaque externe résulterait-elle en une violation de la vie privée de tous ou de certains titulaires de noms de domaine ? Dans quelle mesure serait-il facile d'appliquer des contrôles pour détecter/dissuader les attaques externes ?
- **Cohérence en matière de sécurité :** Dans quelle mesure le modèle est-il vulnérable à une mise en œuvre de sécurité et une imposition de politique incohérentes ? Les buts en matière de sécurité seront-ils uniformément atteints par tous les acteurs responsables de l'opération des composantes du système ? ou bien la sécurité sera grandement affectée par les différences d'expertise et d'investissements des bureaux d'enregistrement/registres/validateurs ?

Incidences sur la juridiction et la vie privée

- **Stocke des données dans les juridictions locales :** Le modèle permet-il un stockage d'informations d'enregistrement dans l'une des multiples juridictions ? Dans quelle mesure les titulaires de ND ou les bureaux d'enregistrement/validateurs pourraient-ils choisir de stocker des informations d'enregistrement dans une juridiction disposant de lois sur la protection des données compatibles avec la juridiction locale du titulaire du ND.
- **Permet l'affichage de l'application des lois locales :** Le modèle permet-il un accès aux informations d'enregistrement de manière compatible avec l'une des multiples juridictions ? Dans quelle mesure le RDS pourrait-il appliquer les lois sur la protection des données de la juridiction locale du titulaire du ND aux informations d'enregistrement auxquelles il est accédé via le RDS ?
- **Permet la conformité aux lois locales sur la protection des données :** Le modèle aide-t-il ou empêche-t-il la conformité du bureau d'enregistrement et du registre aux lois locales sur la protection des données qui s'appliquent à eux ? Dans quelle mesure le modèle rendra-t-il laborieuse l'obtention d'exceptions requises pour permettre la conformité ? Comment le respect des procédures juridiques requises par la loi local du titulaire du ND sera-t-il assuré ?

Accréditation

- **Permet l'accréditation du requérant :** Le modèle permet-il aux utilisateurs souhaitant un accès basé sur objectif à des données sécurisées de demander une accréditation, d'être évalués, de recevoir des identifiants d'accès et de les utiliser pour disposer d'un accès dûment autorisé aux données ? Dans quelle mesure le modèle aide-t-il ou empêche-t-il l'application uniforme et robuste d'un tel processus d'accréditation du requérant ?

  Validation : La rend-il plus facile ? La rend-il moins coûteuse ? Y a-t-il un système qui rende les identifiants sécurisés plus faciles ou moins chers ?
- **Dépister/pénaliser les requérants :** Dans quelle mesure le modèle peut-il préserver les demandes d'accès et les réponses à des fins de détection d'abus d'accès accrédités (c'est-à-dire des actions qui violent les conditions générales d'accès)? Dans quelle mesure le modèle aide-t-il ou empêche-t-il les actions d'imposition de la conformité (par ex. sanctions à l'égard d'utilisateurs non conformes pour dissuader les abus futurs)?
- **Audit :** Le modèle permet-il un audit des demandes d'accès à des données et des réponses, afin d'évaluer l'efficacité du processus d'accréditation et l'accès autorisé aux données ?

Fonctionnement

- **Portail convivial :** Le modèle permet-il une présentation conviviale des informations d'enregistrement affichées via un portail Web ou renvoyées en réponse à des requêtes de protocole ? Dans quelle mesure le modèle soutient-il les principes d'internationalisation (par ex. soutien des jeux de caractères locaux, traduction de la réponse)? Dans quelle mesure le modèle facilite-t-il un affichage cohérent à travers tous les gTLD ?
- **Rapports d'audits aléatoires d'exactitude des données :** Le modèle soutient-il des audits d'exactitude et des rapports d'exactitude réguliers à travers tous les gTLD ? Dans quelle mesure le modèle facilite-t-il une détection et une actualisation efficaces et cohérentes des informations d'enregistrement inexactes ainsi qu'une application uniforme des politiques relatives à l'exactitude ?
- **Temps d'attente des données (performance) :** Le modèle présente-t-il des inefficacités intrinsèques dans le traitement de données, qui pourraient affecter les performances sans pouvoir être réglées à travers une plateforme de mise en œuvre extensible ? Quelle est l'ampleur relative de ces inefficacités (en comparaison avec d'autres modèles) quant à la vitesse de traitement des requêtes et aux retards perçus par les utilisateurs qui demandent ces informations d'enregistrement ?
- **Synchronisation des données :** Le modèle exige-t-il que les données copiées d'un système quelconque soient synchronisées avec d'autres systèmes ? Quelle est l'importance de ces besoins de synchronisation de données et dans quelle mesure un manque provisoire de synchronisation serait-il problématique (en comparaison avec d'autres modèles) ?
- **Accès du titulaire du ND à ses propres données :** Le modèle soutient-il ou empêche-t-il l'accès du titulaire du ND à ses propres données d'enregistrement ?
- **Exigences de stockage/de dépôt de données:** Le modèle introduit-il de multiples zones de stockage qui augmentent le nombre ou la complexité des exigences de stockage et de dépôt des données ?
- **Permet des mesures de prévalidation :** Le modèle soutient-il la prévalidation d'informations de contact de titulaires de ND et de PBC à travers tous les gTLD ? Dans quelle mesure le modèle facilite-t-il une création et maintenance efficaces et cohérentes des informations de contact prévalidées ainsi qu'une application uniforme de politiques relatives à l'unicité ?

Mise en œuvre

- **Infrastructure complexe :** Le modèle est-il moins complexe dans l'ensemble, comparé à d'autres modèles ? Par exemple, un modèle plus complexe (moins puissant) pourrait avoir beaucoup plus de systèmes et d'interfaces qui nécessitent un investissement initial et une maintenance continue.
- **Facilité de mise en œuvre :** Le modèle est-il susceptible d'être plus facile à mettre en œuvre, comparé à d'autres modèles ? Par exemple, un modèle plus difficile (moins puissant) pourrait nécessiter des changements d'un plus grand nombre de systèmes.
- **Facilité de transition :** Dans quelle mesure le modèle facilite-t-il une transition harmonieuse du WHOIS actuel au RDS de nouvelle génération, comparé à d'autres modèles ? Ici, un modèle moins puissant est un modèle qui rend la transition à partir des processus existants, plus difficile pour les utilisateurs, les bureaux d'enregistrement et les registres.

Coût

- **Réduit les coûts d'exploitation du WHOIS pour les bureaux d'enregistrement et les registres :** Le modèle sera-t-il susceptible de réduire les coûts d'exploitation et de maintenance en cours pour les bureaux d'enregistrement et les registres, en comparaison avec le système WHOIS actuel ? Ici, le modèle qui réduit les coûts est considéré plus puissant.
- **Coût de mise en œuvre plus réduit :** Le modèle nécessitera-t-il plus ou moins d'investissement initial global dans une infrastructure et des processus nouveaux/modifiés, comparé à d'autres modèles ? Ici, le modèle avec un coût global de mise en œuvre plus réduit est considéré plus puissant.
- **Requête inverse et WhoWas historique :** Le modèle nécessitera-t-il un investissement supplémentaire pour desservir les requêtes inverses et les recherches de WhoWas historique par les requérants autorisés ? Dans ce cas, un modèle nécessitant un coût total plus réduit pour livrer ces services est considéré plus puissant.

Cas d'utilisation

Comparer la capacité de ces modèles possibles de soutenir tous les utilisateurs et objectifs identifiés dans le rapport initial, y compris (sans y être limité) les cas d'utilisation de gTLD suivants :

- Acquisition de noms de domaine

- Historique d'enregistrement de nom de domaine (y compris le dépistage d'historiques d'enregistrement de tout nom de domaine (WhoWas))
- Noms de domaine de titulaire de ND spécifié (y compris trouver chaque nom de domaine enregistré par un titulaire de ND spécifique (requête inverse du RDS))
- Procédures UDRP
- Examiner les noms de domaine abusifs
- Dissuader les activités malveillantes sur Internet

Analyses des coûts des modèles

Pour examiner la faisabilité de mise en œuvre et les coûts associés aux modèles SRDS et FRDS, l'ICANN a engagé IBM afin de développer une analyse détaillée focalisée sur les différences de coûts entre ces deux modèles de mise en œuvre possibles. IBM a produit un rapport final intitulé « *analyse des coûts des modèles de mise en œuvre de services d'annuaire d'enregistrement (RDS)*[40]*».* Un extrait des conclusions d'IBM, pris de leur rapport, est reproduit ici pour référence.

Approche

Durant les mois de février et de mars 2014, une analyse de coût budgétaire a été réalisée, comparant les mises en oeuvre des modèles synchronisé[41] *et fédéré du RDS. Une approche par étapes a été utilisée :*

- *Étape 1 : Réunir les exigences de base pour chacun des modèles de mise en œuvre.*
- *Étape 2 : Définir et convenir des hypothèses volumétriques principales fournies par l'ICANN et surtout basées sur les rapport de requêtes WHOIS mensuels fournis par les registres de gTLD. Utiliser ces hypothèses pour dériver la charge de travail prévue pour le système et définir une solution de base de haut niveau pour chacun des deux modèles de mise en œuvre.*
- *Étape 3 : Créer un modèle de coût et réaliser une évaluation de coût budgétaire pour chacune des solutions de base.*
- *Étape 4 : Formuler des conclusions.*

Points de départ de l'entreprise

- *Créer une estimation de coût budgétaire pour le « fournisseur/système RDS » central. Les coûts relatifs à l'opérateur de registre ne sont pas estimés.*

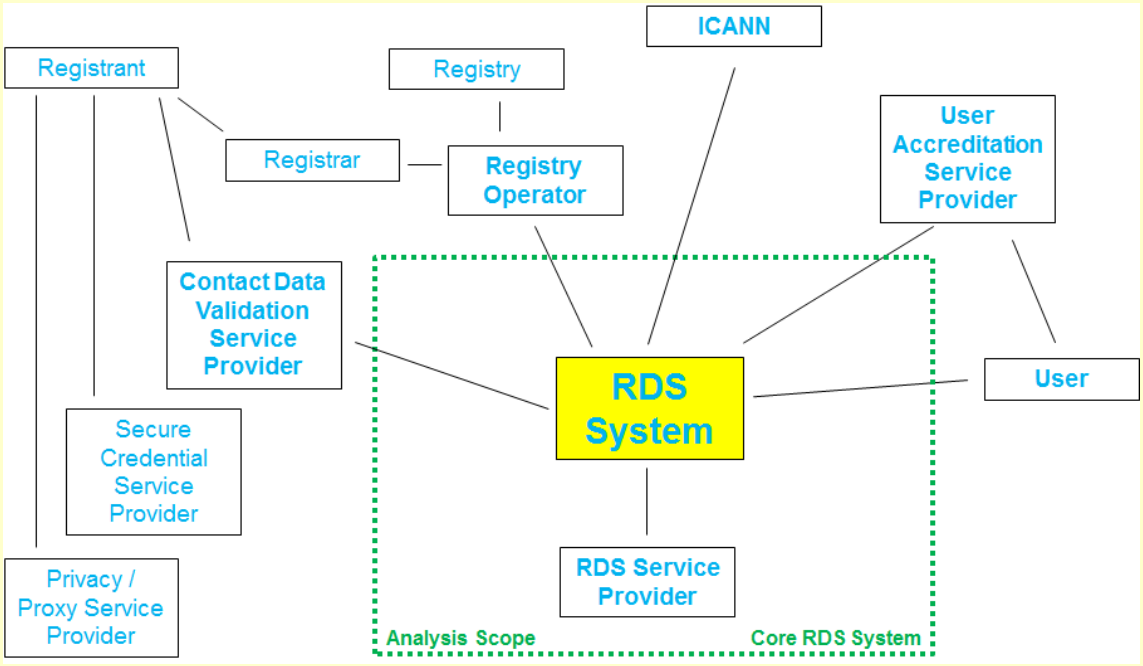
[40] https://community.icann.org/display/WG/EWG+Public+Research+Page

[41] Pour un alignement sur le rapport final de l'EWG, ce résumé se réfère au modèle de RDS synchronisé (SRDS), décrit dans les rapports précédents de l'EWG comme modèle de RDS globalisé (ARDS).

- *Un modèle et une estimation de coût de service géré sont créés. C'est-à-dire, présumer la mise en place et les opérations en cours d'un service de RDS géré et estimer les coûts pertinents.*
- *A des fins de comparaison des coûts, la solution et les coûts sont grandement basés sur le portefeuille d'IBM (surtout l'offre Softlayer IaasS d'IBM), utilisant des composantes de solution de tiers uniquement lorsqu'il n'existe pas d'alternative dans le portefeuille d'IBM.*
- *Les estimations de coût sont créées uniquement pour une ébauche des exigences/solutions de base et non pas pour des variantes ; il n'y a pas eu d'analyse détaillée des éléments de coûts.*

Champ d'analyse principal et données volumétriques

Le point central de l'analyse de coût était le « système RDS principal » tel que décrit ci-dessous.



.

Les cas d'utilisation principaux pour soutenir chacun des modèles (synchronisé et fédéré) ont été définis.

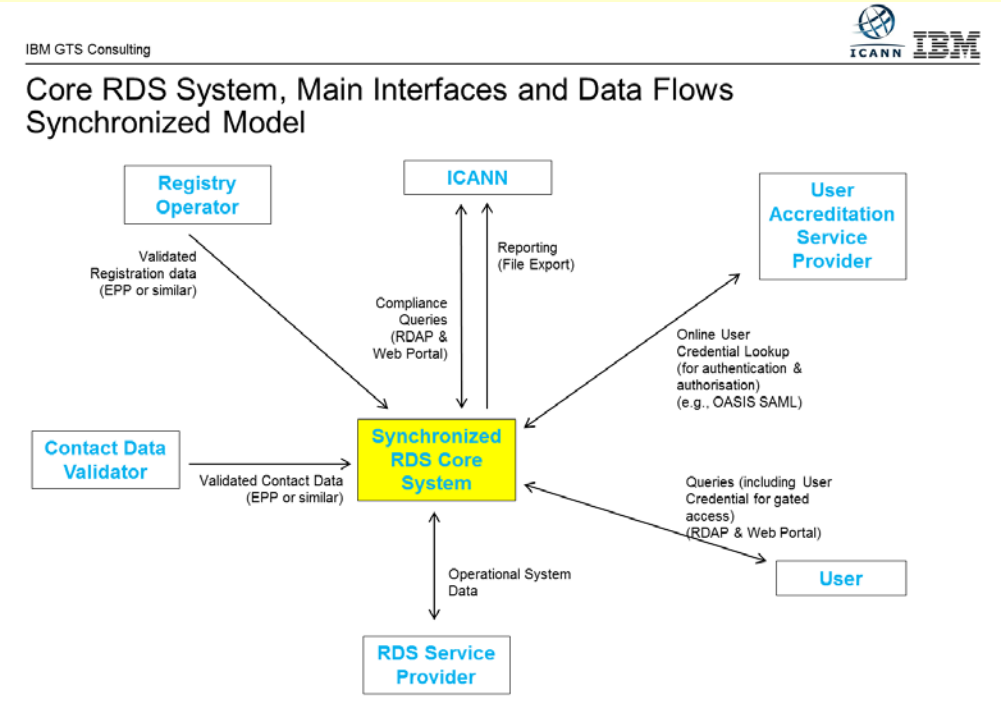
En outre, des hypothèses principales volumétriques ont été définies :

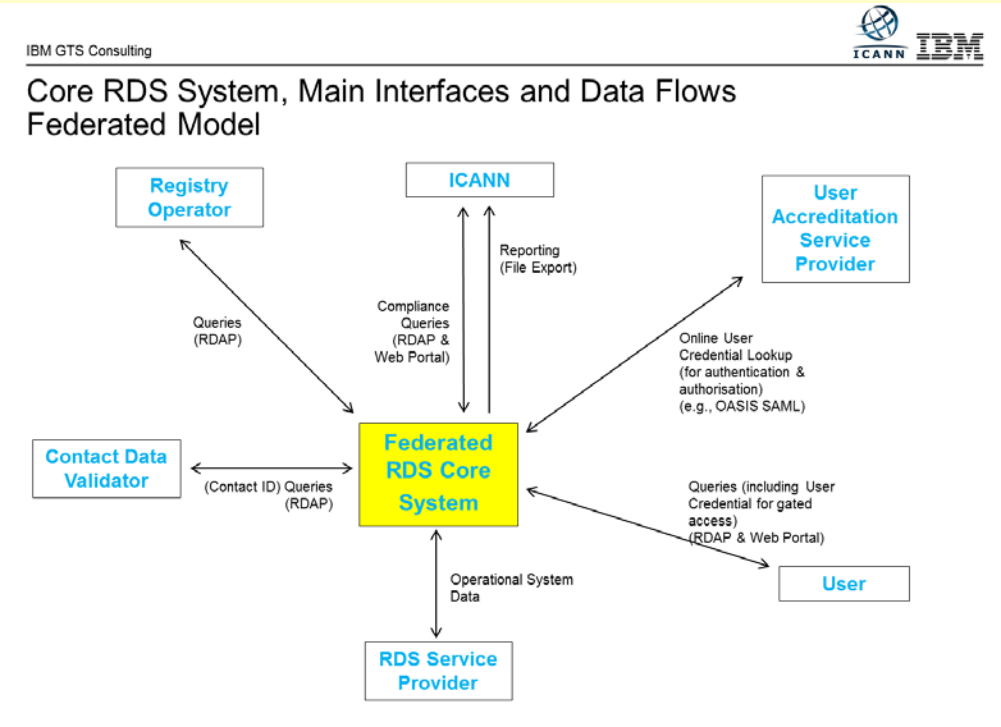
YEARLY GROWTH RATE	22%	nr of DN records added in a year, assumed to include the growth in the nr of gTLDs					
Nr of DN RECORDS, YEARLY UPDATE RATE	100%	nr of DN records updated in a year					
		start yr1 (2015)	start yr2 (2016)	start yr3 (2017)	start yr4 (2018)	start yr5 (2019)	end yr 5 (2020)
	Nr of gTLDs	2000	3000	4000	5000	6000	7000
	growth rate		50%	33%	25%	20%	17%
	December 2013, ICANN input	start yr1 (2015)	start yr2 (2016)	start yr3 (2017)	start yr4 (2018)	start yr5 (2019)	end yr 5 (2020)
NR OF DOMAIN NAMES	151.196.101	184.459.243	225.040.277	274.549.138	334.949.948	408.638.936	498.539.502
NR OF QUERIES/MONTH	9.031.522.529	11.018.457.485	13.442.518.132	16.399.872.121	20.007.843.988	24.409.569.665	29.779.674.992
AVERAGE NR OF QUERIES/SEC	3.484	4.251	5.186	6.327	7.719	9.417	11.489
NR OF QUERIES/PEAK SEC		42.509	51.862	63.271	77.191	94.173	114.891
AVERAGE NR OF QUERIES/HOUR	12.543.781	15.303.413	18.670.164	22.777.600	27.788.672	33.902.180	41.360.660
NR OF QUERIES IN PEAK HOUR	25.087.563	30.606.826	37.340.328	45.555.200	55.577.344	67.804.360	82.721.319
USER VISITS IN PEAK HOUR	16.892.292	20.608.596	25.142.488	30.673.835	37.422.079	45.654.936	55.699.022
CONCURRENT VISITS IN PEAK HOUR	563.076	686.953	838.083	1.022.461	1.247.403	1.521.831	1.856.634
NEW VISITS IN PEAK SEC		28.623	34.920	42.603	51.975	63.410	77.360

% of reverse queries	1,0%

Modèles de mise en œuvre du RDS

Les modèles de mise en œuvre suivants ont été dérivés des rapports initial et de mise à jour de l'EWG aux fins de l'analyse de coût :



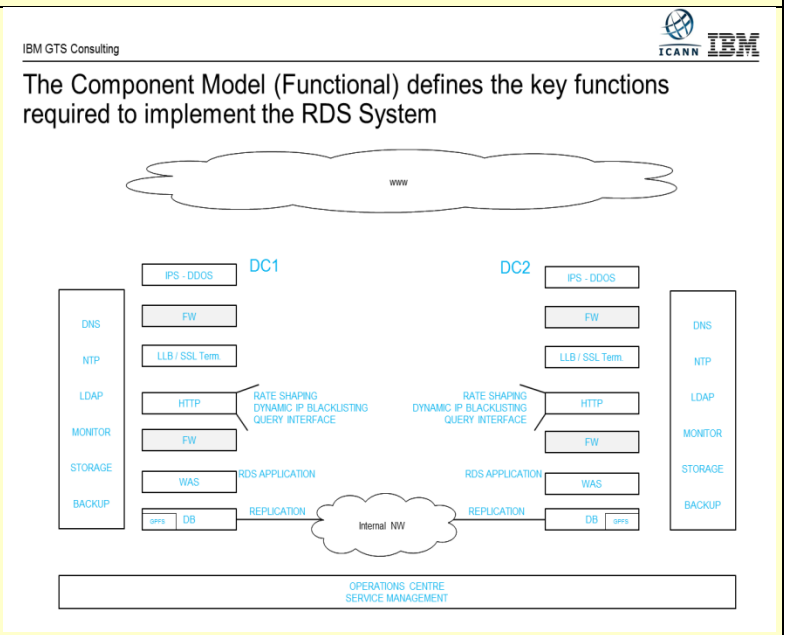


Composantes fonctionnelles du RDS

Le modèle de composantes suivant a été créé à des fins d'analyse de coût, incorporant toutes les fonctions clés requises pour mettre en œuvre le système RDS. Des hypothèses standard de bonnes pratiques dans la conception de systèmes ont été utilisées lors de l'estimation des coûts du SRDS et du FRDS, comme la réplication du système principale du RDS et de la base de données dans deux centres de données géographiquement diversifiés avec un équilibrage de charge et de défaillances pour assurer la redondance et la disponibilité, et détourner les DDoS des FSI. Il faudrait mentionner que ces composantes fonctionnelles S'APPLIQUENT AUX DEUX MODÈLES DE MISE EN OEUVRE.

Composantes fonctionnelles :

- *Équilibrage de charge/routage inter-DC*
- *Réduction des DDoS FSI*
- *Équilibrage de charge et SSL intra-DC*
- *Serveur Web (HTTP)*
- *Serveur applications Web (WAS)*
- *Noeud Admin WAS*
- *Système cache base de données (DB)*
- *Système membres DB*
- *Serveur de stockage*
- *Suivi des systèmes*
- *DNS*
- *NTP*
- *LDSP*
- *Référentiel Syslog*
- *Serveur de sauvegarde*
- *Serveur de stockage de sauvegarde*
- *Système client de sauvegarde DB*
- *Zonage de réseaux, firewall/FSI*
- *Connectivité Internet et DC*



Par exemple, une disposition de deux centres de données a été présumée pour le système principale RDS dans les deux modèles SRDS et FRDS, utilisant une conception active-active où chacun des RDS principaux est capable de traiter 50% de la charge de pointe. Cette analyse de coût n'a pas inclus de regroupement pour une haute disponibilité dans chacun des centres de données ; ceci pourrait être ajouté sans changer les relatifs des deux modèles de RDS.

Estimations de coûts (supposant 1% de requêtes inverses)

L'évaluation de coût résumée ci-dessous ne constitue en aucun manière une proposition de mise en œuvre d'IBM. L'évaluation de coût a été créée dans le seul but et pour la seule utilisation et considération en tant que partie d'une analyse de coût budgétaire visant la comparaison de deux modèles de mise en œuvre de RDS. Sur la base des entrants volumétriques clés, des exigences de charge de travail et des lignes générales des solutions données ci-dessus, les coûts par nom de domaine par année pour les ***systèmes centraux FRDS et SRDS uniquement****, sont estimés à :*

Estimation de coût budgétaire SRDS

€	0,0183	average cost/domain/year

cost per domain name				
yr1	yr2	yr3	yr4	yr5
€ 0,041	€ 0,023	€ 0,017	€ 0,020	€ 0,019

Estimation de coût budgétaire FRDS

€	0,0173	average cost/domain/year

cost per domain name				
yr1	yr2	yr3	yr4	yr5
€ 0,041	€ 0,018	€ 0,017	€ 0,021	€ 0,017

Les différences dans les coûts étaient analysées et comparées comme suit :

FRDS – SRDS Budgetary Cost Estimate Differences

SETUP COSTS		**5,9%**		10,5%	
INFRASTRUCTURE SETUP COSTS	ARCHITECTURE & DESIGN	**1,5%**	0,2%	15,6%	0,0%
	PROVISION & CONFIGURE		1,2%		19,2%
	INFRASTRUCTURE TESTING		0,1%		18,4%
APPLICATION SETUP COSTS	ANALYSIS, DESIGN, CODE, UNIT TEST	**1,2%**	1,2%	0,0%	0,0%
TESTING	INTEGRATION TESTING & DEPLOYMENT	**1,7%**	0,8%	7,8%	0,0%
	E2E SYSTEM TESTING		0,2%		38,2%
	PERFORMANCE		0,2%		33,3%
	SECURITY (ETHICAL HACK)		0,5%		0,0%
TRANSITION TO BAU	TRANSITION TO BAU	**0,6%**	0,5%	26,6%	37,7%
	SERVICE DESK SETUP		0,1%		0,0%
MANAGEMENT	PROJECT MANAGEMENT	**0,9%**	0,9%	13,4%	13,4%

The FRDS model implies a higher computing power requirement (more systems required to handle the envisaged load) in the web and web application server layer.

Due to a higher amount of systems to interface with in an on-line manner when handling queries, the FRDS model is estimated to involve more testing effort

FRDS – SRDS Budgetary Cost Estimate Differences

COST MODEL FRDS		SHARE IN TOTAL		DIFFERENCE WITH ARDS	
		100,0%		-5,4%	
RUN COSTS		94,1%		-6,3%	
INFRASTRUCTURE COSTS	PUBLIC NW	**30,5%**	8,1%	-22,4%	-55,9%
	DC NW, GLB, LLB, IPS/DDOS		5,7%		10,7%
	HTTP SERVERS		2,2%		236,0%
	WAS SERVERS		3,7%		218,5%
	DB SERVERS		2,2%		-52,0%
	STORAGE		6,3%		-3,8%
	BACKUP		1,9%		-19,0%
	GENERIC SYSTEMS		0,3%		0,0%
SW LICENCE & MAINTENANCE COSTS	DB	**32,7%**	13,7%	-17,5%	-59,5%
	WAS		18,8%		234,6%
	BACKUP		0,3%		0,0%
OPERATIONS AND MANAGEMENT COSTS	INFRA OPERATIONS & MAINTENANCE	**30,9%**	19,4%	44,0%	63,6%
	APPLICATION OPERATIONS		2,6%		20,0%
	APPLICATION MAINTENANCE		1,3%		27,3%
	SERVICE GOVERNANCE		5,2%		0,0%
	SERVICE DESK		2,4%		100,0%

The Public NW cost is lower in the FRDS case due to the IBM SoftLayer NW charging model: incoming traffic is free; per server 20 TB/month outgoing traffic is free, i.e. you get a total free outgoing volume of #servers x 20 TB per month. As the number of servers increases in the FRDS model, the total amount of free TB outgoing NW volume/month increases.

The FDRS model implies a higher NW throughput requirement. Impact on Firewall and Intrusion Prevention Component.

The FRDS model implies a higher computing power requirement in the web and web application server layer.

The FRDS model implies less storage and backup storage capacity as less data is stored centrally.

The DB compute requirement is estimated to be higher in the SRDS model.

Due to a higher amount of systems to interface with in an on-line manner when handling queries, the FRDS model is estimated to involve a higher application operations, support & maintenance release testing workload

Conclusions principales

Avec les hypothèses utilisées, le système RDS central est légèrement moins cher dans le modèle RDS fédéré (FRDS) que dans le modèle RDS synchronisé (SRDS).

Le modèle FRDS est très sensible aux variations de charge des requêtes inverses. Avec un plus grand nombre de requêtes inverses, le modèle FRDS devient sensiblement plus cher : avec 3% de charge de requêtes inverses au lieu de 1% de charge de requêtes inverses, le coût du modèle FRDS devient 35% plus cher. Il s'agit d'un facteur d'incertitude et de risque important associé au modèle FRDS. Le modèle SRDS, au contraire, est estimé moins sensible au nombre de requêtes inverses.

Le modèle FRDS nécessiterait probablement des opérations, un soutien, une maintenant et des efforts d'essais plus élevés comme l'on prévoit plus d'interactions avec les opérateurs de registres.

En outre, le modèle FRDS a plus d'impact sur les opérateurs de registres. Dans le modèle FRDS, chaque opérateur de registre devra mettre en place un soutien - sous SLA - pour les requêtes en ligne, y compris les requêtes inverses et les requêtes concernant les propriétaires successifs (à savoir WhoWas). Pour ces dernières, les données historiques devraient également être maintenues par les opérateurs de registres.

ANNEXE G : CAPACITÉ DES PROTOCOLES EPP ET RDAP À SOUTENIR LE RDS

Élément de données	Soutien EPP pour la collecte	Soutien RDAP pour l'accès
Nom de domaine	Y	Y
Statut de l'enregistrement	Y	Y
Serveurs DNS	Y	Y
Délégation DNSSEC	Y	Y
Statut du client	Y	Y
Statut du serveur	Y	Y
Bureau d'enregistrement	Y	Y
Revendeur	Y	Y
Juridiction du bureau d'enregistrement	N	N
Juridiction du registre	N	N
Langue de l'accord d'enregistrement	N	Y
Date de création	Y	Y
Date de l'enregistrement initial	Y	Y
Date d'expiration du bureau d'enregistrement	Y	Y
Type de titulaire de nom de domaine	N	Y*
Nom du PBC	Y	Y
ID du PBC	Y	Y
Statut de validation du PBC	N	N
Horodatage dernière validation du PBC	N	N
Organisation du PBC	Y	Y
Adresse de résidence du PBC	Y	Y
Ville du PBC	Y	Y
État / province du PBC	Y	Y
Code postal du PBC	Y	Y
Pays du PBC	Y	Y
Adresse électronique du PBC	Y	Y
Adresse électronique alternative du PBC	N	Y
Numéro de poste téléphonique du PBC	Y	Y
Numéro de poste téléphonique alternatif du PBC	N	Y
Numéro de poste télécopie du PBC	Y	Y
Messagerie texte du PBC	N	Y
Messagerie instantanée du PBC	N	Y
Médias sociaux du PBC, médias sociaux	N	Y

Élément de données	Soutien EPP pour la collecte	Soutien RDAP pour l'accès
alternatifs		
URL de contact et en cas d'abus du PBC	N	Y
Date de mise à jour	Y	Y
Nom du titulaire du nom de domaine	Y	Y
ID de contact du titulaire du nom de domaine	Y	Y
Statut de validation du contact du titulaire du nom de domaine	N	N
Horodatage dernière validation du contact du titulaire du nom de domaine	N	N
Organisation du titulaire du nom de domaine	Y	Y
Identifiant de l'entreprise du titulaire du ND	Y	Y
Adresse de résidence du titulaire du nom de domaine	Y	Y
Ville du titulaire du nom de domaine	Y	Y
État / province du titulaire du nom de domaine	Y	Y
Code postal du titulaire du nom de domaine	Y	Y
Pays du titulaire du nom de domaine	Y	Y
Numéro de poste téléphonique du titulaire du nom de domaine	Y	Y
Numéro de poste de télécopie du titulaire du nom de domaine	Y	Y
Adresse électronique, adresse électronique alternative du titulaire du nom de domaine	Y	Y
Messagerie texte du titulaire de nom de domaine	N	Y
Messagerie instantanée du titulaire de nom de domaine	N	Y
Médias sociaux du titulaire du nom de domaine, médias sociaux alternatifs	N	Y
URL de contact et en cas d'abus du titulaire du nom de domaine	N	Y

Élément de données	Soutien EPP pour la collecte	Soutien RDAP pour l'accès
URL du bureau d'enregistrement	N	Y
Numéro IANA du bureau d'enregistrement	N	Y*
Adresse électronique de contact avec le bureau d'enregistrement en cas d'abus	N	Y
Numéro de téléphone de contact avec le bureau d'enregistrement en cas d'abus	N	Y
URL du site de plaintes Internic	N	Y

*Ces éléments de données ne sont pas clairement spécifiés dans le RDAP. Ils peuvent être renvoyés en utilisant des champs « remarques » ou une extension de protocole.

Extensions et/ou ajouts de protocoles

Juridiction du bureau d'enregistrement et du registre : Aurait besoin d'être ajoutée à l'EPP ou dérivée des informations de l'emplacement actuel du bureau d'enregistrement. Peut être renvoyé utilisant les « remarques » entité du RDAP ou via une extension de protocole.

Langue de l'accord d'enregistrement : Aurait besoin d'être ajoutée à l'EPP par l'extension de protocole.

Type de titulaire de nom de domaine : Aurait besoin d'être ajouté à l'EPP par l'extension de protocole.

Statut de validation titulaire/PBC, horodatage dernière validation, email alternatif, poste téléphonique alternatif, SMS, IM, médias sociaux, médias sociaux alternatifs, URL de contact, URL en cas d'abus : Auraient besoin d'être ajoutés à l'EPP par l'extension de protocole. Le RDAP peut traiter des identifiants de médias sociaux, mais une spécification aurait besoin d'être créée pour définir le format de ces identifiants.

Type de contact : Les types actuellement disponibles sont « admin. », « facturation » et « tech. » Des types de contact supplémentaires nécessiteraient une extension du RDAP.

Objectif énoncé dans une requête RDAP : Aurait besoin d'être ajouté au RDAP par l'extension de protocole.

Niveau d'accès dans l'EPP : L'EPP comprend un mécanisme simple de collecte et de transfert des préférences de divulgation d'éléments de contact du titulaire du ND du bureau d'enregistrement au registre, où elles peuvent être utilisées pour guider le

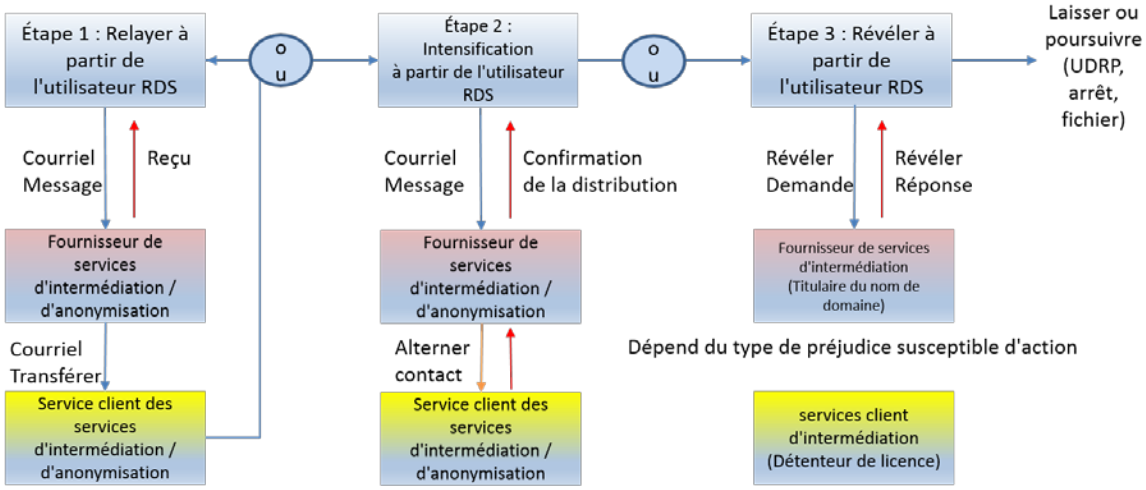
comportement de réponse du RDAP. Cependant, ce mécanisme n'est pas assez fin pour capter les préférences au niveau de chaque élément de donnée individuel. Une nouvelle extension EPP et/ou mis en correspondance du contact seraient donc nécessaires pour indiquer le choix du titulaire du ND ou du contact et passer outre les caractéristiques de divulgation par défaut de chaque élément de donnée (par ex. choisir de publier un élément sécurisé par défaut).

ANNEXE H : MODÈLE ET PRINCIPES POUR LE RELAIS ET LA DIVULGATION

Tel que noté dans la section VI(b), l'EWG recommande que les services accrédités d'anonymisation/d'intermédiation soient obligés de transmettre tous les emails reçus par l'adresse de transmission d'email. Le but est de fournir aux clients des services accrédités d'anonymisation/d'intermédiation et aux utilisateurs du RDS qui souhaiteraient les contacter, une voie de communication standard, toujours disponible, en quasi temps réel.

De plus, l'EWG recommande d'exiger des services d'intermédiation de répondre aux demandes de divulgation de manière opportune (voir détails ci-dessous). Le but est de fournir aux utilisateurs qui ont des problèmes graves avec des domaines enregistrés par intermédiation, un processus standard, toujours disponible et efficace de chercher une solution efficace à leur problème.

En analysant ces besoins d'utilisateurs, l'EWG a noté une autre insuffisance dans les pratiques actuelles : l'absence d'une méthode de remontée facilement disponible, efficace lorsque la communication échoue. Plusieurs utilisateurs passent rapidement à la divulgation parce qu'il n'ont pas d'autre recours. L'EWG recommande la mise en place d'un processus de remontée qui peut être moins coûteux pour tous et réduire le nombre de problèmes qui conduisent à des demandes de divulgation coûteuses et longues. Ce processus à trois étapes est illustré ci-dessous :



Étape 1 : Relais

a) L'utilisateur du RDS demande des données de contact d'un domaine, extrayant :

- L'ID de contact du titulaire du ND (c'est-à-dire l'ID de contact du client d'anonymisation ou du fournisseur d'intermédiation)

- Les ID de contact de tous les PBC obligatoires et les adresses publiées des PBC (y compris les adresses email)

- Une indication que l'enregistrement du domaine a été faite via service P/P et

- Nom et adresse du fournisseur accrédité de services d'anonymisation ou d'intermédiation, fournis comme PBC de ce fournisseur et comportant des URL publiés de formulaires de remontée de relais et de divulgation.

b) L'utilisateur du RDS, notant qu'il s'agit d'un enregistrement par service accrédité d'anonymisation/d'intermédiation, essaye d'envoyer un courriel à l'adresse de transmission du client d'anonymisation/d'intermédiation. Les fournisseurs peuvent facultativement choisir de laisser leurs clients fournir plus d'une adresse de transmission (par ex. téléphone, SMS, portail).

c) Le fournisseur accrédité d'anonymisation/d'intermédiation doit être tenu de transmettre et d'accuser réception du message transmis (par ex. accusé de réception de tous les messages reçus pour l'adresse de transmission d'emails). Un accusé négatif peut être renvoyé en cas d'erreur (par ex. une telle boîte de messagerie n'existe pas) et les accusés de réception au même expéditeur pourraient être limités à un certain seuil pour dissuader les abus de transmission.

d) L'utilisateur du RDS recevant l'accusé de réception a donc une confirmation que le message a été transmis au client d'anonymisation/d'intermédiation. Cependant, le client peut choisir de ne pas répondre ou d'ignorer le message transmis sans le lire (par ex. le considérer comme pourriel).

Étape 2 : Remontée

L'utilisateur du RDS est fatigué d'attendre une réponse du client des services accrédités P/P et décide d'intensifier le contact tenté précédemment en :

a) Visitant le site Web du service accrédité d'anonymisation ou d'intermédiation identifié dans l'étape 1 et de remplir un formulaire de remontée qui contient :

- l'identité de l'utilisateur du RDS (éventuellement en réutilisant un identifiant de requête du RDS)

- le motif de l'utilisateur du RDS pour le contact (pourrait être un menu déroulant de motifs définis)

- le nom de domaine enregistré par anonymisation/intermédiation.
- un message téléchargé à transmettre au client (éventuellement crypté ?)
- l'horodatage de la première tentative de transmission

b) Le fournisseur accrédité de services d'anonymisation/d'intermédiation doit être tenu d'essayer de contacter le client directement, en utilisant éventuellement des informations de contact et/ou des méthodes inaccessibles à l'utilisateur du RDS, renvoyant une « confirmation de livraison » dans les N*[42] jours. Ici aussi, des confirmations négatives seraient renvoyées dans le cas d'erreur (par ex. utilisateur non authentifié, expiration de session) et les soumissions pourraient être inscrites et limitées par un seuil afin de dissuader les abus.

d) L'utilisateur du RDS recevant la confirmation a donc une preuve que le message a été transmis au client d'anonymisation/d'intermédiation. Le client peut toujours choisir de ne pas répondre, mais la remontée doit aider à dépasser les échecs de communication de base sans nécessiter de divulgation.

Étape 3 : Divulgation (s'applique uniquement aux domaines enregistrés par intermédiation)

Le temps s'écoule pendant que l'utilisateur du RDS attend que le client du Proxy accrédité (détenteur de licence) réponde et décide que le problème est assez important pour procéder à une action policière ou en justice en :

a) Visitant le site Web du service ou appelant ou envoyant un courriel au fournisseur accrédité d'intermédiation identifié dans l'étape 1 et en soumettant une demande de divulgation qui contient :

- l'identité de l'utilisateur du RDS
- le motif de l'utilisateur du RDS pour le contact (étroitement limité aux préjudices susceptibles d'action)
- le nom de domaine enregistré par intermédiation
- la documentation du préjudice (informations d'enregistrement de marque déposée, allégations d'abus)

[42] * L'expiration de session peut dépendre de l'identité authentifiée et du motif de contact énoncé. Par exemple, 1 jour pour les représentants de la loi et les OpSec enquêtant sur un crime/un abus ; 7 jours pour les propriétaires de marques enquêtant sur une violation de marque de commerce ; 7 jours pour les consommateurs Internet essayant de joindre des marchands en ligne.

- l'horodatage de la tentative de transmission/remontée (numéro de cas de remontée ?)

b) Le fournisseur accrédité de services d'intermédiation doit être tenu d'enquêter et de prendre les mesures appropriées (voir d), renvoyant une « réponse de divulgation » dans les N*[43] jours. Les demandes de divulgation pourraient être inscrites et limitées aux préjudices susceptibles d'action allégués par les utilisateurs du RDS avec leur rang,[44] pour dissuader les abus.

c) Le fournisseur accrédité d'intermédiation, ayant la documentation pouvant servir à évaluer le cas, pourrait :

- notifier et transférer le domaine au client (c'est-à-dire interrompre le service d'intermédiation)
- suspendre le domaine provisoirement durant une enquête policière
- divulguer à l'utilisateur l'identité/le contact d'un détenteur de licence engagé dans des activités illégales
- refuser la divulgation – affirmant positivement sa responsabilité en matière d'utilisation future du domaine.

Une politique doit être élaborée pour décrire en détail ce qui constitue une documentation suffisante et quand le détenteur de licence doit être notifié. En outre, il y aura besoin de politiques claires concernant l'impact des lois et des facteurs locaux à considérer. Tout ce qui précède se passe aujourd'hui, sans aucune supervision, directive de politique ou conséquences en cas de refus/d'ignorance de divulgation.

d) L'utilisateur du RDS recevant la réponse de divulgation a maintenant l'information nécessaire pour abandonner l'affaire ou poursuivre par une action en justice. Par exemple, la violation de marque de commerce pourrait conduire à la déposition d'une UDRP, alors qu'une enquête policière pourrait conduire à l'arrestation d'un suspect. Si la divulgation est refusée (ou la réponse opportune n'est pas reçue),

---

[43] * L'expiration de session peut dépendre du requérant et du motif de contact énoncé. Les représentants de la loi pourraient directement aller à l'étape 3 (divulgation) pour des enquêtes urgentes. Les cadres temporels et les efforts pour l'étape 2 doivent être assez réduits pour décourager les autres de passer directement à l'étape 3.

[44] ** Tout utilisateur demandant une divulgation doit démontrer qu'il est ou qu'il représente une partie victime d'un préjudice susceptible d'action. Par exemple, les détenteurs de marques ou leurs agents alléguant une violation de marque déposée pourraient montrer qu'ils possèdent un ou des noms de domaine similaires à celui enregistré par intermédiation. Une réflexion plus approfondie est nécessaire pour tracer un lien entre les types d'utilisateurs et les types de préjudices. Voir la liste de GoDaddy d'options de formulaires de plaintes relatives à des domaines enregistrés par intermédiation, comme exemple.

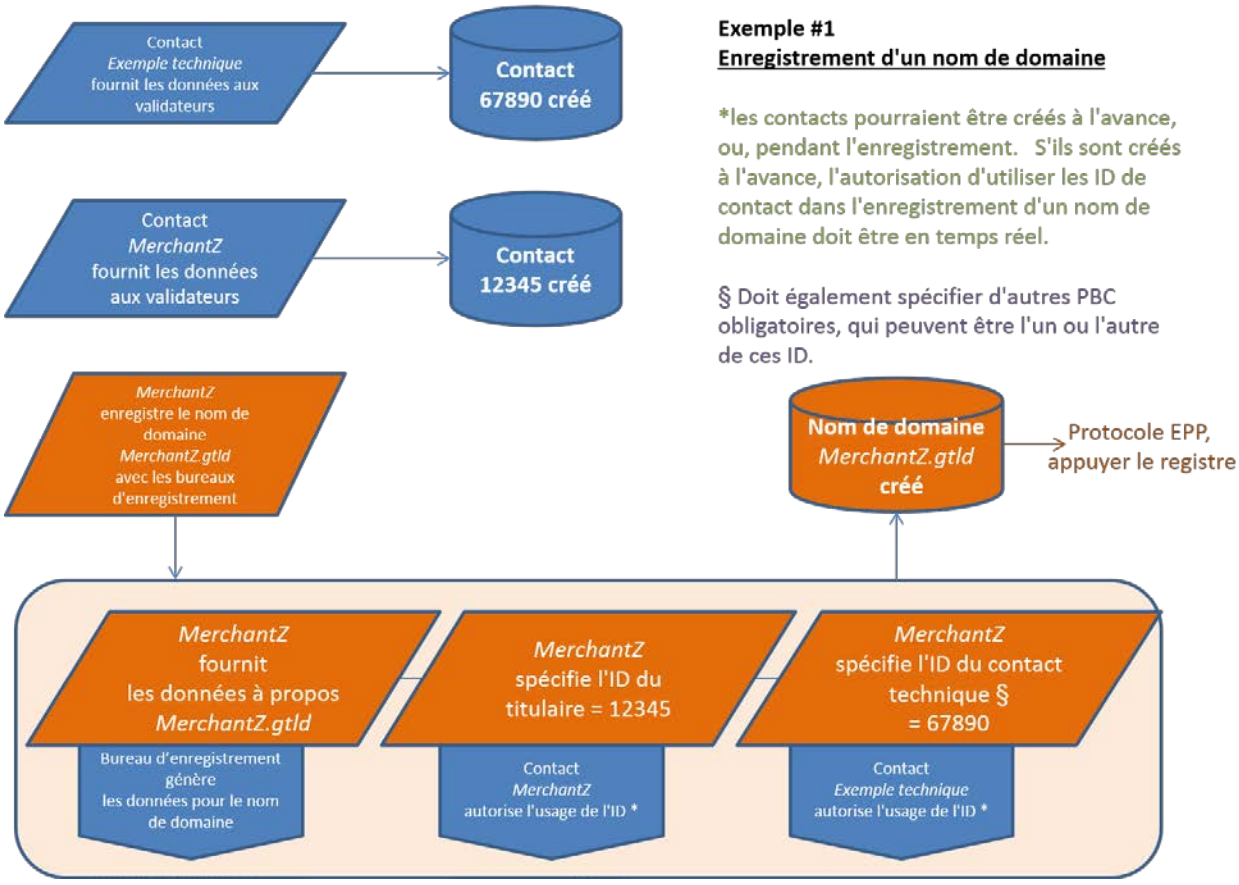
l'utilisateur du RDS peut maintenant aussi choisir d'intenter une action en justice contre le fournisseur d'intermédiation accrédité.

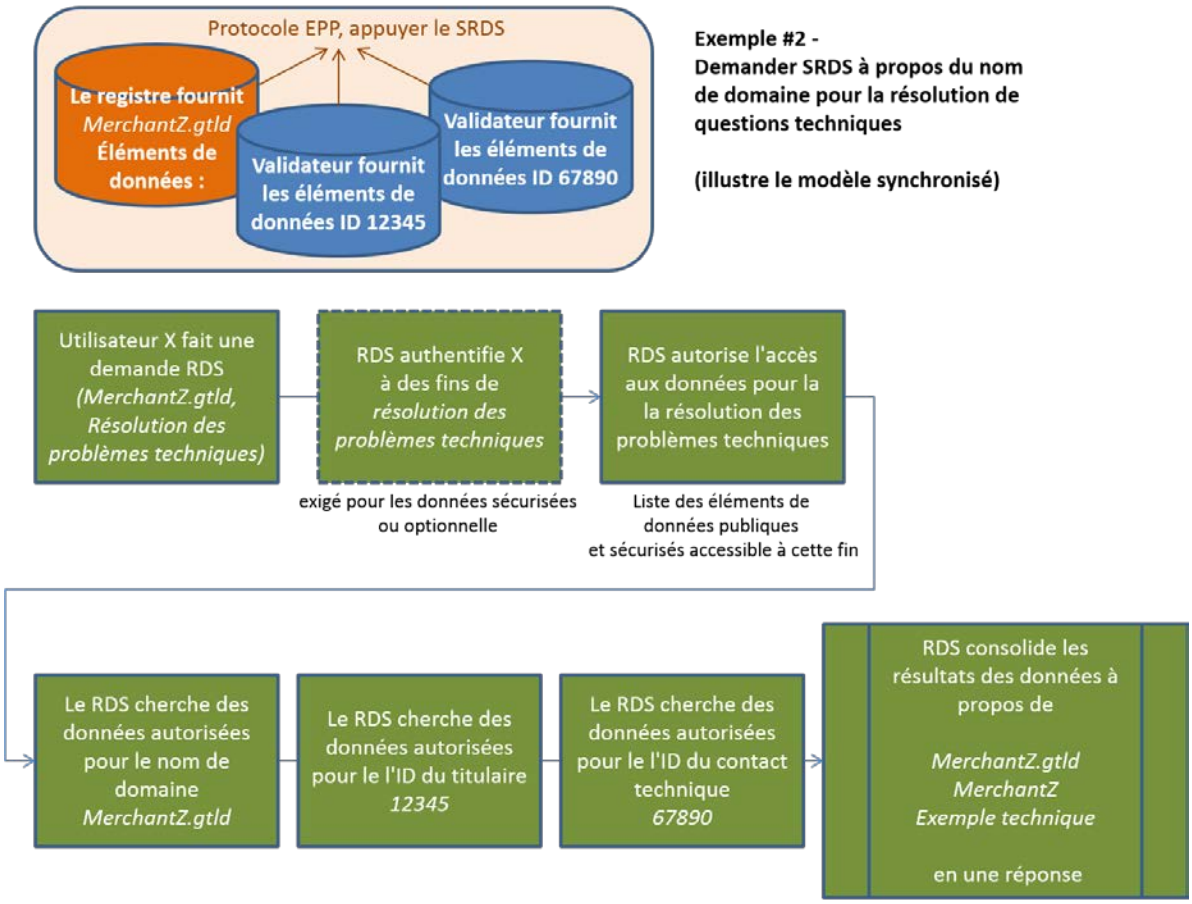
Il faudrait noter que les procédures décrites ci-dessus ne traitent pas le cas où un enregistrement par anonymisation ou intermédiation doit être « démasqué » au public plutôt que simplement « divulgué » au requérant.

Ces modèles et processus suggérés doivent être encore affinés par le groupe de travail PPSAI de la GNSO, en se basant sur l'examen des besoins de la communauté de l'ICANN et en étant guidés par les bonnes pratiques identifiées par des réponses à l'enquête en ligne de l'EWG sur les fournisseurs de services d'anonymisation et d'intermédiation.

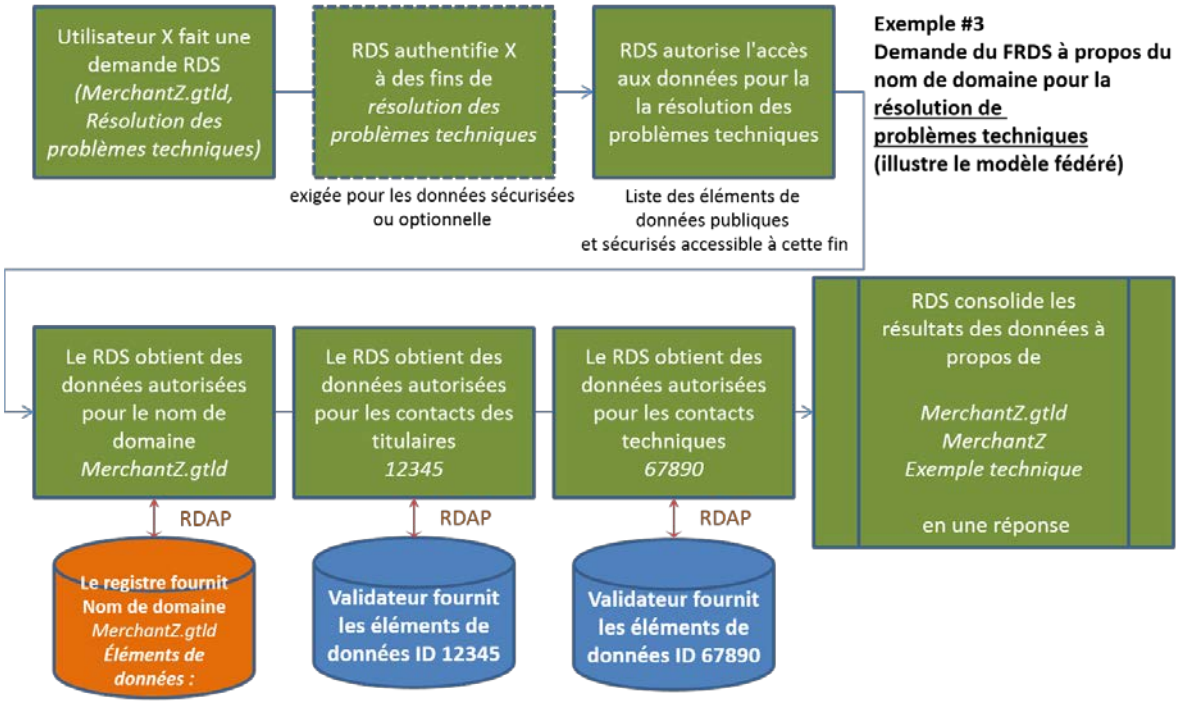
ANNEXE I : SCHÉMAS OPÉRATIONNELS DU RDS

Les représentations graphiques suivantes illustrent les flux de données clés entre les acteurs de l'écosystème du RDS durant l'enregistrement de noms de domaine et les requérant demandant des informations au RDS à propos de ces noms de domaine pour résoudre des questions d'ordre technique.





Pour faciliter la comparaison des modèles, le même exemple est répété ci-dessous pour le FRDS.



ANNEXE J : À PROPOS DE L'EWG

Processus de sélection et vision

En réunissant l'EWG, le Conseil d'administration de l'ICANN a adopté une nouvelle approche pour résoudre une question difficile qui a connu plusieurs années de surplace et de discorde. Le Conseil d'administration a réuni des individus représentant un large éventail de perspectives et de parties prenantes dans l'espoir qu'en partageant leur expertise, ils puissent réussir là où d'autres ont échoué. Par la remise du présent rapport

final et de ses 180 principes appuyés par consensus, la vision du Conseil d'administration s'est effectivement matérialisée.

Les membres de l'EWG ont été soigneusement sélectionnés avec l'aide d'un facilitateur expérimenté et neutre, M. Jean-Francois Baril. Il a été choisi à cause de son expérience dans l'élaboration de normes dans le secteur de l'électronique grand public. Des douzaines de candidatures à l'EWG ont été examinées sur la base de plusieurs critères, y compris les capacités de leadership, l'expertise, la diversité géographique, l'établissement de consensus, l'aptitude à innover et, dans certains cas, la neutralité. Il a été estimé que des individus extérieurs à la communauté de l'ICANN pourraient apporter une perspective intacte, non défraichie par des tentatives précédentes de traiter la question du WHOIS.

Composition de l'EWG

L'EWG est composé d'individus, de chargés de liaison du Conseil et de membres du personnel d'Australie, du Canada, de Chine, de la commission européenne, d'Irlande, de Jamaïque, du Nigeria, de Norvège, de Suisse, du Royaume-Uni et des États-Unis. Cette diversité géographique a prouvé être essentielle à la compréhension des nombreux défis juridictionnels associés au travail de l'EWG.

Les membres de l'EWG comprenaient des entrepreneurs expérimentés et des leaders mondiaux (Ajayi, Ala-Pietilä, Neylon, Rasmussen et Shah). Leur expérience collective dans l'équilibrage des risques et leur résolution de problèmes en fonction des résultats ont tracé la voie qui a permis de parvenir à une concertation précoce au sein de l'EWG.

Comme le mandat de l'EWG comprenait l'examen de politiques publiques, notamment de questions de vie privée, l'expertise spécifique dans le secteur du gouvernement était essentielle à son succès. Perrin et Niebel ont apporté leur expérience d'un point de vue canadien et français, garantissant que ces questions étaient au premier plan dans la conception du système de nouvelle génération. Il est important de noter que, durant ses délibérations, l'EWG a été mise au courant et a essayé de tenir compte des derniers développement en matière de législation sur la protection des données dans l'union européenne.

Un autre aspect critique du travail de l'EWG comprenant le fait de veiller à ce que ses recommandations soient raisonnablement applicables dans le cadre de l'écosystème actuel du DNS. L'expertise des membres du bureau d'enregistrement de gTLD (Neylon), du registre gTLD (Hollenbeck-.com and .net), et des ccTLD (.cn-Jian, .uk-Nanayakkara, .ng- Ajayi et .au-Disspain) a éclairé des questions telles que les approches de validation,

les enregistrements par anonymisation/intermédiation, la compatibilité avec des protocoles tels que l'EPP et le nouveau RDAP en cours de développement par l'IETF, ainsi que l'incorporation de concepts tels que « l'accès sécurisé » pour l'affichage d'éléments de données sensibles.

Les questions de sécurité et de stabilité ont également été examinées, tirant parti de la perspicacité de membres actuels et précédents du SSAC (Crocker et Rasmussen), qui ont contribué par leur compréhension étendue des besoins des représentants de la loi dans la lutte contre les abus malveillants impliquant le DNS.

La conception d'un nouveau système est impossible sans la prise en considération des besoins des multiples utilisateurs du RDS de nouvelle génération. L'EWG a inclus des membres jouissant d'une connaissance profonde des questions de propriété intellectuelle (Kawaguchi, Vayra et Shah) qui se fient fortement au système du WHOIS actuel pour lutter contre le cybersquattage, la fraude et la contrefaçon en ligne, ainsi que des perspectives partagées avec des utilisateurs finaux (Samuels et Phifer). Ces perspectives variées ont aidé à s'assurer que les objectifs légitimes pour un accès RDS aux données d'enregistrement seraient desservis, tout en réduisant au minimum les inefficacités et les abus des processus d'enregistrement actuels dans la mesure du possible.

Pour conforter l'EWG, les membres du personnel de l'ICANN (Michel, Milam) ont apporté leur perspicacité exécutive et leur savoir en matière de cadre contractuel de l'ICANN. Un consultant (Phifer) a également fourni des données des études approfondies du WHOIS réalisées par la GNSO au cours des dernières cinq années afin d'aider l'EWG à formuler des recommandations basées sur des faits.

Méthodologie de travail

L'EWG a entamé son travail par une série d'activités visant à mieux se connaitre mutuellement dans le but de privilégier les rapports, la confiance et, surtout, le sentiment d'appartenir à une équipe. L'EWG a établi une série de valeurs d'équipe pour surmonter les obstacles éventuels à l'exploration de solutions innovatrices à ce problème complexe. Il s'agit des valeurs suivantes :

- Dans cette équipe en tant qu'individus
- S'exprimer librement
- Pas d'attribution de médias sociaux
- Honnêteté intellectuelle
- Auto-réglementation sectorielle
- Conception à partir de zéro

- Prise en compte des dures réalités (technologie et gouvernements)

Ces valeurs ont aidé à guider l'EWG vers les compromis nécessaires pour concevoir le RDS et produire les principes exposés dans le présent rapport final.

Pour plus d'informations et les biographies des membres de l'EWG, veuillez consulter cette annonce.