Internet Engineering Task Force (IETF)
Request for Comments : 8499
BCP : 219
RFC rendue obsolète : 7719
RFC mise à jour : 2308
Catégorie : Bonnes pratiques actuelles
ISSN : 2070-1721

P. Hoffman, ICANN
A. Sullivan
K. Fujiwara, JPRS
janvier 2019

Traduction Claude Brière de L'Isle

Terminologie du DNS

Résumé
Le système des noms de domaines (DNS, *Domain Name System*) est défini dans des douzaines de RFC différentes. La terminologie utilisée par les mises en œuvre et les développeurs de protocoles du DNS, et par les opérateurs des systèmes du DNS, a parfois changé depuis les dizaines d'années écoulées depuis la première définition du DNS. Le présent document donne dans un seul document les définitions actuelles pour beaucoup des termes utilisés dans le DNS.

Le présent document rend obsolète la RFC 7719 et met à jour la RFC 2308.

Statut de ce mémoire
Le présent mémoire documente les bonnes pratiques actuelles de l'Internet.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Tous les documents approuvés par l'IESG ne sont pas candidats à devenir une norme de l'Internet ; voir la Section 2 de la RFC7841.

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à http://www.rfc-editor.org/info/rfc8499.

Table des matières

1. Introduction

Le système des noms de domaines (DNS) est un simple protocole d'interrogation-réponse dont les messages dans les deux directions ont le même format. (La Section 2 donne une définition de "DNS public", qui est souvent ce que veulent dire les gens quand ils parlent du "DNS".) Le protocole et le format de message sont définis dans la [RFC1034] et la [RFC1035]. Ces RFC ont défini certains termes, et des document ultérieurs en ont défini d'autres. Certains des termes provenant des [RFC1034] et [RFC1035] ont aujourd'hui des significations assez différentes de celles qu'elles avaient en 1987.

Le présent document contient une collection d'une large variété de termes relatifs au DNS, organisés en gros par thème. Certains d'entre eux ont été définis avec précision dans des RFC antérieures, d'autres ont été vaguement définis dans ces RFC antérieures, et certains n'étaient pas définis du tout.

D'autres organisations définissent parfois de leur propre chef des termes relatifs au DNS. Par exemple, le groupe de travail WHAT définit "domaine" à <https://url.spec.whatwg.org/>. Le comité consultatif du système de serveur racine (RSSAC, *Root Server System Advisory Committee*) a un bon lexique [RSSAC026].

La plupart des définitions qui figurent ici représentent le consensus de la communauté du DNS -- à la fois des développeurs de protocole et des opérateurs. Certaines des définitions diffèrent de celles de RFC antérieures, et ces différences sont notées. Dans le présent document, lorsque le consensus sur la définition est le même que celui d'une RFC, cette RFC est citée. Lorsque le consensus sur la définition a un peu changé, la RFC est mentionnée mais la nouvelle définition autonome est donnée. Voir à l'Appendice A la liste des définitions que met à jour le présent document.

Il est important de noter que, durant le développement du présent document, il est devenu clair que certains termes relatifs au DNS sont interprétés de façon assez différente par différents experts du DNS. De plus, certains termes qui sont définis dans les premières RFC du DNS ont maintenant une définition sur laquelle il y a un accord général, mais qui est différente de la définition d'origine. Donc, le présent document est une révision substancielle de la [RFC7719].

Noter qu'il n'y a pas qu'une seule définition cohérente "du DNS". Il peut être considéré comme étant une combinaison d'un schéma de dénominations couramment utilisé pour les objets sur l'Internet, une base de données répartie qui représente les noms et certaines propriétés de ces objets, une architecture qui assure la maintenance, la résilience, et une vague cohérence réparties pour cette base de données, et un simple protocole de questions-réponses (comme mentionné plus loin) qui met en œuvre cette architecture. La Section 2 définit le "DNS mondial" et le "DNS privé" comme moyen de traiter ces différences de définition.

L'utilisation des majuscules dans les termes du DNS est souvent peu cohérente entre les RFC et les divers praticiens du DNS. L'utilisation des majuscules dans le présent document est un pari sur les pratiques actuelles, et n'est pas destinée à indiquer que les autres styles de mise en majuscule sont erronés ou archaïques. Dans certains cas, plusieurs styles de mise en majuscule sont utilisés pour le même terme à cause de la citation de RFC différentes.

Le lecteur devrait noter que les termes dans ce document sont groupés par sujets. Ceux qui ne sont pas déjà familiarisés avec le DNS ne vont probablement pas pouvoir tout savoir sur le DNS en lisant le présent document du début à la fin. Se promener à l'intérieur du document pourrait peut-être être la seule façon de voir assez de contexte pour comprendre certaines définitions. L'index qui se trouve à la fin du document pourrait être utile pour les lecteurs qui tentent d'en savoir plus sur le DNS par la lecture de ce document.

2. Noms

Système de dénomination *(naming system)* : un système de dénomination associe les noms aux données. Les systèmes de dénomination ont de nombreuses facettes significatives qui aident à les différencier les unes des autres. Certaines des facettes couramment identifiées sont :

* la composition des noms
* le format des noms

* l'administration des noms
* les types de données qui peuvent être associés aux noms
* les types de métadonnées pour les noms
* le protocole pour obtenir des données à partir d'un nom
* le contexte pour la résolution d'un nom

Noter que cette liste est un petit sous ensemble des facettes que les gens ont identifiées au fil du temps pour les systèmes de dénomination, et l'IETF doit encore se mettre d'accord sur beaucoup des facettes qui peuvent être utilisées pour comparer les systèmes de dénomination. Par exemple, d'autres facettes pourraient inclure les "protocoles pour metttre à jour les données dans un nom", la "confidentialité des noms", et la "confidentialité des données associées aux noms", mais elles ne sont pas aussi bien définies que celles énumérées ci-dessus. La liste qu'on donne ici a été choisie parce qu'elle aide à décrire le DNS et les systèmes de dénomination similaires au DNS.

Nom de domaine *(Domain name)* : liste ordonnée d'une ou plusieurs étiquettes.
Noter que cette définition est indépendante des RFC du DNS ([RFC1034] et [RFC1035]), et que cette définition s'applique aussi aux systèmes autres que le DNS. La [RFC1034] définit un "espace de noms de domaines" en utilisant des arborescences mathématiques et leurs nœuds dans la théorie des graphes, et cette définition a le même résultat pratique que notre définition. Tout chemin d'un graphe acyclique dirigé peut être représenté par un nom de domaine consistant en les étiquettes de ses nœuds, ordonnés par distance décroissante depuis la ou les racines (ce qui est la convention normale au sein du DNS, y compris dans ce document). Un nom de domaine dont la dernière étiquette identifie une racine du graphe est pleinement qualifiée ; les autres noms de domaines dont les étiquettes forment un strict préfixe d'un nom de domaine pleinement qualifié sont relatifs à ce premier nœud omis.

Noter aussi que différents documents de l'IETF et autres ont utilisé le terme de "nom de domaine" de nombreuses façons différentes. Il est courant dans les premiers documents d'utiliser "nom de domaine" pour signifier "noms qui correspondent à la syntaxe de la [RFC1035]", mais éventuellement avec des règles supplémentaires telles que "et sont, ou seront, résolvables dans le DNS mondial" ou "mais seulement en utilisant le format de présentation".

Étiquette *(Label)* : liste ordonnée de zéro, un ou plusieurs octets qui constituent une portion d'un nom de domaine. En utilisant la théorie des graphes, une étiquette identifie un nœud dans une portion du graphe de tous les noms de domaines possibles.

DNS mondial *(Global DNS)* : en utilisant le petit ensemble de facettes citées sous "Système de dénomination", le DNS mondial peut être défini comme suit. La plupart des règles données ici proviennent des [RFC1034] et [RFC1035], bien que le terme "DNS mondial" n'ait pas été défini jusqu'à présent.

Composition des noms : un nom a une ou plusieurs étiquettes dans le DNS mondial. La longueur de chaque étiquette est entre 0 et 63 octets inclus. Dans un nom de domaine pleinement qualifié, la dernière étiquette dans la liste ordonnée est longue de 0 octet ; c'est la seule étiquette dont la longueur peut être de 0 octet, et elle est appelée la "racine" ou "étiquette racine". Un nom de domaine dans le DNS mondial a une longueur maximum totale de 255 octets dans le format du réseau ; la racine représente un octet pour ce calcul. (Le DNS en diffusion groupée [RFC6762] permet des noms de jusqu'à 255 octets plus un octet de terminaison sur la base d'une interprétation différente de la RFC 1035 et de ce qui est inclus dans les 255 octets.)

Format des noms : les noms dans le DNS mondial sont des noms de domaines. Il y a trois formats : le format du réseau, le format de présentation, et l'affichage courant. Le format de base du réseau pour les noms dans le DNS mondial est une liste d'étiquettes ordonnées par distance décroissante de la racine, avec l'étiquette racine en dernier. Chaque étiquette est précédée d'un octet de longueur. La [RFC1035] définit aussi un schéma de compression qui modifie ce format. Le format de présentation pour les noms dans le DNS mondial est une liste d'étiquetttes ordonnées par distance décroissante de la racine, codées en ASCII, avec un caractère "." entre chaque étiquette. Dans le format de présentation, un nom de domaine pleinement qualifié inclut l'étiquette racine et les points de séparation associés. Par exemple, dans le format de présentation, un nom de domaine pleinement qualifié avec deux étiquettes non racines est toujours montré comme "exemple.tld." au lieu de "exemple.tld". La [RFC1035] définit une méthode pour montrer les octets qui ne s'affichent pas en ASCII. Le format d'affichage courant est utilisé dans les applications et le texte libre. Il est le même que le format de présentation, mais en montrant l'étiquette racine et le "." avant elle est facultatif et il est rarement montré. Par exemple, en format d'affichage courant, un nom de domaine pleinement qualifié avec deux étiquettes non racines est généralement montré comme "exemple.tld" au lieu de "example.tld.". Les noms dans le format d'affichage courant sont normalement écrits de telle sorte que la directionnalité du système d'écriture présente les étiquettes par distance décroisante de la racine (de sorte que aussi bien en français que dans le langage de programmation C, l'étiquette racine ou de domaine de niveau supérieur (TLD, *Top-Level Domain*) est la plus à droire dans la liste ordonnée, mais en arabe, elle peut être la plus à gauche, selon les conventions locales).

Administration des noms : l'administration est spécifiée par délégation (voir la définition de "délégation" à la Section 7). Les politiques pour l'administration de la zone racine dans le DNS mondial sont déterminées par la communauté opérationnelle des dénominations, qui se réunit dans le cadre de la corporation Internet pour l'allocation des noms et des numéros (ICANN, *Internet Corporation for Assigned Names and Numbers*). La communauté opérationnelle des dénominations choisit l'opérateur des fonctions de IANA pour la zone racine du DNS mondial. Au moment de la rédaction du présent document, cet opérateur est "Identifiants techniques publics" (PTI, *Public Technical Identifiers*). (Voir à <https://pti.icann.org/ > plus d'informations sur la réalisation par PTI des fonctions de l'IANA.) Les serveurs de noms qui servent la zone racine sont fournis par des opérateurs racine indépendants. Les autres zones dans le DNS mondial ont leurs propres politiques d'administration.

Type de données qui peuvent être associés aux noms : un nom peut avoir zéro, un ou plusieurs enregistrements de ressources associés. Il y a de nombreux types d'enregistrements de ressource avec des structures de données uniques définis dans de nombreuses RFC différentes et dans le registre de l'IANA à [IANA-RR].

Types de métadonnées pour les noms : tout nom qui est publié dans le DNS apparaît comme un ensemble d'enregistrements de ressources (voir la définition de "RRset" à la Section 5). Certains noms ne le font pas, ayant eux-mêmes des données associés dans le DNS, mais ils "apparaissent" de toutes façons dans le DNS parce que ils font partie d'un nom plus long qui n'a pas de données associées (voir la définition de "vides non terminaux" à la Section 7).

Protocole pour obtenir des données à partir d'un nom : le protocol décrit dans la [RFC1035].

Contexte pour résoudre un nom : la zone racine du DNS mondial distribuée par PTI.

DNS privé : noms qui utilisent le protocole décrit dans la [RFC1035] mais qui ne s'appuient pas sur la zone racine du DNS mondial ou noms qui sont par ailleurs non généralement disponibles sur l'Internet mais utilisent le protocole décrit dans la [RFC1035]. Un système peut utiliser à la fois le DNS mondial et un ou plusieurs systèmes de DNS privés ; par exemple, voir "DNS partagé" à la Section 6.
Noter que les noms de domaines qui n'apparaissent pas dans le DNS, et qui sont destinés à n'être jamais l'objet de recherches avec le protocole du DNS, ne font pas partie du DNS mondial ni d'un DNS privé même si ce sont des noms de domaines.

DNS en diffusion groupée (mDNS, *Multicast DNS*) : le "DNS en diffusion groupée (mDNS) donne la capacité d'effectuer des opérations comme celles du DNS sur la liaison locale en l'absence de tout serveur DNS conventionnel en envoi individuel. De plus, le DNS en diffusion groupée désigne une portion de l'espace de noms du DNS qui est d'utilisation locale libre, sans avoir besoin de payer de redevance annuelle, et sans qu'il soit besoin d'établir des délégations ou par ailleurs de configurer un serveur DNS conventionnel pour répondre à ces noms." (Cité de la [RFC6762], Résumé). Bien qu'il utilise un format réseau compatible, le mDNS est, strictement parlant, un protocole différent du DNS. Aussi, lorsque la citation ci-dessus dit "une portion de l'espace de noms du DNS", il serait plus clair de dire "une portion de l'espace des noms de domaines". Les noms dans le mDNS ne sont pas destinés à faire l'objet de recherches dans le DNS.

Zone DNS à desserte locale *(Locally served DNS zone)* : une zone DNS à desserte locale est un cas particulier de DNS privé. Les noms sont résolus en utilisant le protocole DNS dans un contexte local. La [RFC6303] définit des sous domaines de IN-ADDR.ARPA qui sont des zones de desserte locales. La résolution des noms à travers des zones de desserte locale peut avoir des résultats ambigus. Par exemple, le même nom peut se résoudre en résultats différents dans des contextes de zone DNS de desserte locale différentes. Le contexte pour une zone DNS à desserte locale peut être explicite, comme celles qui sont énumérées dans les [RFC6303] et [RFC7793], ou implicite, comme celles définies par l'administration DNS locale et ne sont pas connues pour le client de résolution.

Nom de domaine pleinement qualifié (FQDN, *Fully-Qualified Domain Name*) : c'est souvent juste une façon claire de dire la même chose que "nom de domaine d'un nœud", comme mentionné plus haut. Cependant, le terme est ambigu. Strictement parlant, un nom de domaine pleinement qualifié devrait inclure chaque étiquette, incluant l'étiquette de longueur zéro de la racine : un tel nom serait écrit "www.exemple.net." (noter le point de terminaison). Mais, parce que tous les noms partagent finalement la racine commune, les noms sont souvent écrits par rapport à la racine (comme "www.exemple.net") et sont quand même appelés "pleinement qualifiés". Ce terme est apparu pour la première fois dans la [RFC0819]. Dans le présent document, les noms sont souvent écrits par rapport à la racine.
Le besoin du terme "nom de domaine pleinement qualifié" vient de l'existence de noms de domaines partiellement qualifiés, qui sont des noms où une ou plusieurs des dernières étiquettes dans la liste ordonnée sont omises (par exemple, un nom de domaine de "www" relatif à "exemple.net" identifie "www.exemple.net"). De tels noms relatifs ne sont compris que par leur contexte.

Nom d'hôte *(Host name)* : ce terme et son équivalent, "nom_d'hôte" a été largement utilisé mais pas défini dans les [RFC1034],

[RFC1035], [RFC1123], ou [RFC2181]. Le DNS était à l'origine déployé dans l'environnement du tableau des hôtes comme indiqué dans la [RFC0952], et il est probable que le terme a suivi de façon informelle de cette définition. Au fil du temps, la définition semble avoir évolué. "Nom d'hôte" est souvent compris comme étant un nom de domaine qui suit les règles du paragraphe 3.5 de la [RFC1034], qui sont aussi appelées la "syntaxe préférée de nom". (Dans cette syntaxe, chaque caractère de chaque étiquette est une lettre, un chiffre, ou un tiret). Noter que toute étiquette dans un nom de domaine peut contenir toute valeur d'octet ; les noms d'hôtes sont généralement considérés comme étant des noms de domaines dans lesquels chaque étiquette suit les règles de la "syntaxe préférée de nom", avec l'amendement que les étiquettes peuvent commencer par des chiffres ASCII (cet amendement vient du paragraphe 2.1 de la [RFC1123]).
Les gens utilisent parfois aussi le terme "nom_d'hôte" pour se référer à la seule première étiquette d'un FQDN, comme à "imprimante" dans "imprimante.admin.exemple.com". (Parfois, cela est formalisé dans la configuration dans les systèmes d'exploitation.) De plus, les gens utilisent parfois ce terme pour décrire tout nom qui se réfère à une machine, et cela peut inclure des étiquettes qui ne se conforment pas à la "syntaxe préférée de nom".

Domaine de niveau supérieur (TLD, *Top-Level Domain*) : un domaine de niveau supérieur est une zone qui est une couche en dessous de la racine, comme "com" ou "jp". Il n'y a rien de particulier à dire du point de cue du DNS, sur les TLD. La plupart d'entre eux sont aussi des zones de centre de délégation (définies à la Section 7) et il y a des problèmes significatifs au sujet de leur fonctionnement. Les TLD sont souvent divisés en sous groupes comme les domaines de niveau supérieur de code de pays (ccTLD), les domaines génériques de niveau supérieur (gTLD), et autres ; la division est une affaire de politique et sort du domaine d'application de ce document.

Nom de domaine internationalisé (IDN, *Internationalized Domain Name*) : le protocole d'application des noms de domaines internationalisés (IDNA, *Internationalized Domain Names for Applications*) est le mécanisme standard pour traiter les noms de domaines avec des caractères non ASCII dans les applications du DNS. La norme actuelle au moment de la rédaction de ce document, normalement appelée "IDNA2008", est définie dans les [RFC5890], [RFC5891], [RFC5892], [RFC5893], et [RFC5894]. Ces documents définissent de nombreux termes spécifiques de IDN, tels que "étiquette LDH", "étiquette A", et "étiquette U". La [RFC6365] définit plus de termes qui se rapportent à l'internationalisation (dont certains se rapportent aux IDN) ; la [RFC6055] a une discussion plus large des IDN, incluant une nouvelle terminologie.

Sous domaine *(subdomain)* : "Un domaine est un sous domaine d'un autre domaine si il est contenu au sein de ce domaine. Cette relation peut être vérifiée en regardant si le nom du sous domaine se termine par le nom du domaine contenant." (Cité de la [RFC1034], paragraphe 3.1). Par exemple, dans le nom d'hôte "nnn.mmm.exemple.com", "mmm.exemple.com" et "nnn.mmm.exemple.com" sont tous deux des sous domaines de "exemple.com". Noter que les comparaisons sont faites ici sur les étiquettes entières ; c'est-à-dire que, "ooo.exemple.com" n'est pas un sous domaine de "oo.exemple.com".

Alias : propriétaire d'un enregistrement de ressource CNAME, ou sous domaine du propriétaire d'un enregistrement de ressource DNAME (les enregistrements DNAME sont définis dans la [RFC6672]). Voir aussi "nom canonique".

Nom canonique *(Canonical name)* : un enregistrement de ressource CNAME "identifie son nom de propriétaire comme un alias, et spécifie le nom canonique correspondant dans la section RDATA du RR". (Cité de la [RFC1034], paragraphe 3.6.2). Cet usage du mot "canonique" se rapporte au concept mathématique de "forme canonique".

CNAME : "Il est traditionnel de se référer au [propriétaire] d'un enregistrement CNAME comme à "un CNAME". C'est dommage car "CNAME" est l'abréviation de "nom canonique", et le [propriétaire] d'un enregistrement CNAME n'est très certainement pas un nom canonique." (Cité de la [RFC2181], paragraphe 10.1.1. Le texte cité a été changé de "étiquette" en "propriétaire".)

3. Codes de réponse du DNS

Certains des codes de réponse (RCODE) qui sont définis dans la [RFC1035] ont acquis leurs propres noms abrégés. Tous les RCODE sont données à [IANA-RR], bien que cette liste utilise une casse mixte, alors que la plupart des documents utilisent une forme toute en majuscules. Certains des nom courants pour les valeurs définies dans la [RFC1035] sont décrits dans cette section. Elle comporte aussi un RCODE supplémentaire et une définition générale. La liste officielle de tous les RCODE est dans le registre de l'IANA.

NOERROR : ce RCODE apparait comme "condition de non erreur" au paragraphe 4.1.1 de la [RFC1035].

FORMERR : ce RCODE apparaît comme "erreur de format - le serveur de noms a été incapable d'interpréter l'interrogation" au paragraphe 4.1.1 de la [RFC1035].

SERVFAIL : ce RCODE apparaît comme "échec du serveur - le serveur de noms a été incapable de traiter cette interrogation à cause d'un problème du serveur de noms" au paragraphe 4.1.1 de la [RFC1035].

NXDOMAIN : ce RCODE apparaît comme "Erreur de nom [...] ce code signifie que le nom de domaine référencé dans l'interrogation n'existe pas." au paragraphe 4.1.1 de la [RFC1035]. La [RFC2308] établit NXDOMAIN comme synonyme de "Erreur de nom".

NOTIMP : ce RCODE apparaît commse "Non mis en œuvre - le serveur de noms ne prend pas en charge le type d'interrogation demandé" au paragraphe 4.1.1 de la [RFC1035].

REFUSED : ce RCODE apparaît comme "Refusé - le serveur de noms refuse d'effectuer l'opération spécifiée pour des raisons de politique. Par exemple, un serveur de noms peut ne pas souhaiter fournir les informations à ce demandeur particulier, ou un serveur de noms peut ne pas souhaiter effectuer une certaine opération (par exemple, un transfert de zone) pour certaines données." au paragraphe 4.1.1 de la [RFC1035].

NODATA : "Pseudo RCODE qui indique que le nom est valide, pour la classe en question, mais il n'y a pas d'enregistrement de ce type. Une réponse NODATA doit être déduite de la réponse." (Cité de la [RFC2308], Section 1) "NODATA est indiqué par une réponse avec le RCODE réglé à NOERROR et aucune réponse pertinente dans la section Réponse. La section Autorité va contenir un enregistrement SOA, ou il n'y aura pas d'enregistrement NS." (Cité de la [RFC2308], paragraphe 2.2). Noter que les points de référence ont un format similaire aux réponses NODATA ; la [RFC2308] explique comment les distinguer.
Le terme "NXRRSET" est parfois utilisé comme synonyme de NODATA. C'est cependant une faute, étant donné que NXRRSET est un code d'erreur spécifique défini dans la [RFC2136].

Réponse négative *(Negative response)* : réponse qui indique qu'un RRset particulier n'existe pas ou dont le RCODE indique que le serveur de noms ne peut pas répondre. Les Sections 2 et 7 de la [RFC2308] décrivent en détails les types de réponse négative.

4. Transactions du DNS

L'en-tête d'un message du DNS est ses 12 premiers octets. Beaucoup des champs et fanions des diagrammes des paragraphes 4.1.1 à 4.1.3 de la [RFC1035] sont désignés par leur nom dans chaque diagramme. Par exemple, les codes de réponse sont appelés des "RCODE", les données pour un enregistrement sont appelélees des "RDATA", et le bit de réponse d'autorité est souvent appelé le "fanion AA" ou le "bit AA".

Classe : une classe "identifie une famille de protocoles ou une instance d'un protocole". (Cité de la [RFC1034], paragraphe 3.6) "Le DNS marque toutes les données avec une classe ainsi que le type, de sorte qu'on puisse permettre l'usage en parallèle de différents formats pour les données d'adresse de type." (Cité de la [RFC1034], paragraphe 2.2). En pratique, la classe pour presque toutes les interrogations est "IN" (l'Internet). Il y a quelques interrogations pour "CH" (la classe Chaos), mais elles sont généralement à des fins d'information sur le serveur lui-même plutôt que pour un type d'adresse différent.

QNAME : la définition la plus couramment utilisée est que le QNAME est un champ dans la section Question d'une interrogation. "Une interrogation standard spécifie un nom de domaine cible (QNAME), un type d'interrogation (QTYPE), et une classe d'interrogation (QCLASS) et demande des RR qui correspondent." (Cité de la [RFC1034], paragraphe 3.7.1). Strictement parlant, la définition vient du paragraphe 4.1.2 de la [RFC1035], où le QNAME est défini par rapport à la section Question. Cette définition apparaît être appliquée de façon cohérente : la discussion des interrogations inverses au paragraphe 6.4.1 se réfère au "nom du propriétaire du RR d'interrogation et son TTL", parce que les interrogations inverses remplissent la section Réponse et laissent la section Question vide. (Les interrogations inverses sont déconseillées dans la [RFC3425] ; et donc, les définitions pertinentes n'apparaissent pas dans ce document.)

Cependant, la [RFC2308] a une autre définition qui met le QNAME dans la réponse (ou série de réponses) au lieu de l'interrogation. Elle définit le QNAME comme "...le nom dans la section interrogation d'une réponse, ou là où cela se résout en un CNAME, ou une chaîne de CNAME, le champ de données du dernier CNAME. Le dernier CNAME dans ce sens est ce qui contient une valeur qui ne se résout pas en un autre CNAME." Cette définition a une certaine logique interne, à cause de la façon dont fonctionne la substitution de CNAME et de la définition de CNAME. Si un serveur de noms ne trouve pas un RRset qui corresponde à une interrogation, mais trouve le même nom dans la même classe avec un enregistrement CNAME, alors le serveur de noms "inclut l'enregistrement de CNAME dans la réponse et recommence l'interrogation au nom de domaine spécifié dans le champ de données de l'enregistrement CNAME." (Cité du paragraphe 3.6.2 de la [RFC1034]) Cela est rendu explicite dans l'algorithme de résolution présenté au paragraphe 4.3.2 de la

[RFC1034], qui dit de "changer le QNAME en le nom canonique dans le RR CNAME, et revenir à l'étape 1" dans le cas d'un RR CNAME. Car un enregistrement CNAME déclare explicitement que le nom du propriétaire est désigné canoniquement avec ce qui est dans les RDATA, il y a alors un moyen de voir le nouveau nom (c'est-à-dire, le nom qui était dans les RDATA du RR CNAME) comme étant aussi le QNAME.

Cependant, cela crée une sorte de confusion parce que la réponse à une interrogation qui résulte en un traitement de CNAME contient en écho dans la section Question un QNAME (le nom dans l'interrogation d'origine) et un second QNAME qui est dans le champ Données du dernier CNAME. La confusion vient du mode de résolution itératif/récurrent, qui retourne finalement une réponse qui n'a en fait pas besoin d'avoir le même nom de propriétaire que le QNAME contenu dans l'interrogation d'origine.

Pour régler cette potentielle confusion, il est utile de distinguer trois significations :

* QNAME (original) : le nom réellement envoyé dans la section Question de l'interrogation d'origine, qui est toujours en écho dans la réponse (finale) dans la section Question lorsque le bit QR est établi à 1.
* QNAME (effectif) : un nom effectivement résolu, qui est soit le nom interrogé à l'origine, soit un nom reçu dans une réponse de chaîne de CNAME.
* QNAME (final) : le nom réellement résolu, qui est soit le nom réellement interrogé, soit alors le dernier nom d'une réponse de chaîne de CNAME.

Noter que parce que la définition de la [RFC2308] est en fait pour un concept différent de celui de la [RFC1034], il aurait été mieux que la [RFC2308] utilise un nom différent pour ce concept. Dans l'usage général d'aujourd'hui, QNAME signifie presque toujours ce qui est défini ci-dessus comme "QNAME (original)".

Point de référence *(Referral)* : type de réponse dans lequel un serveur, signalant qu'il n'est pas (pas complètement) d'autorité pour une réponse, fournit au résolveur qui l'interroge un autre endroit auquel envoyer son interrogation. Les points de référence peuvent être partiels.

Un point de référence survient quand un serveur n'effectue pas un service récurrent lorsque il répond à une interrogation. Il apparaît à l'étape 3(b) de l'algorithme du paragraphe 4.3.2 de la [RFC1034].

Il y a deux types de réponses de point de référence. Le premier est un point de référence vers le bas (parfois décrit comme une "réponse de délégation") où le serveur est d'autorité pour une portion du QNAME. La section d'autorité des RDATA du RRset contient les serveurs de noms spécifiées à la coupure de zone référencée. Dans le fonctionnement normal du DNS, cette sorte de réponse est requise afin de trouver les noms derrière une délégation. L'utilisation simple de "point de référence" signifie cette sorte de point de référence, et de nombreuses personnes croient que c'est la seule sorte de point de référence légitime dans le DNS.

Le second est un point de référence vers le haut (parfois décrit comme un "point de référence racine") quand le serveur n'est pas d'autorié pour toutes les portions du QNAME. Quand cela arrive, la zone à laquelle on se réfère dans la section d'autorité est généralement la zone racine ("."). Dans le fonctionnement normal du DNS, cette sorte de réponse n'est pas exigée pour la résolution ou pour répondre correctement à toute interrogation. Il n'est pas exigé qu'un serveur envoie des points de référence vers le haut. Certains considèrent les points de référence vers le haut comme le signe d'une mauvaise configuration ou d'une erreur. Les points de référence vers le haut ont toujours besoin d'un qualificatif (comme "vers le haut" ou "racine") et ne sont jamais identifiés simplement par le mot "point de référence".

Une réponse qui a seulement un point de référence contient une section de réponse vide. Elle contient le RRset NS pour la zone de référence dans la section Autorité. Elle peut contenir des RR qui fournissent des adresses dans la section supplémentaire. Le bit AA est à zéro.

Dans le cas où l'interrogation correspond à un alias, et où le serveur n'est pas d'autorité pour la cible de l'alias mais est d'autorité pour un nom au dessus de la cible de l'alias, l'algorithme de résolution va produire une réponse qui contient à la fois la réponse d'autorité pour l'alias et un point de référence. Une telle réponse partielle et de point de référence a des données dans la section Réponse. Elle a le RRset NS pour la zone de référence dans la section Autorité. Elle peut contenir des RR qui fournissent des adresses dans la section supplémentaire. Le bit AA est établi, parce que le premier nom dans la section Réponse correspond au QNAME et que le serveur est d'autorité pour cette réponse (voir la [RFC1035], paragraphe 4.1.1).

5. Enregistrements de ressource

RR : acronyme de enregistrement de ressource *(resource record)*. (Voir le paragraphe 3.6 de la [RFC1034].)

RRset : ensemble d'enregistrements de ressource "avec la même étiquette, classe et type, mais des données différentes" (selon la [RFC2181], Section 5). Aussi écrit "RRSet" dans certains documents. Pour préciser, "même étiquette" dans cette définition signifie "même nom de propriétaire". De plus, la [RFC2181] déclare que "les TTL de tous les RR dans un RRSet doivent être les mêmes".

Noter que les enregistrements de ressource RRSIG ne correspondent pas à cette définition. La [RFC4035] dit : "Un RRset PEUT avoir plusieurs RR RRSIG associés". Noter que comme les RR RRSIG sont étroitement liés aux RRsets dont ils contiennent les signatures, les RR RRSIG, à la différence de tous les autres types de RR du DNS, ne forment pas de RRsets. En particulier, les valeurs de TTL parmi les RR RRSIG avec un nom de propriétaire commun ne suivent pas les règles de RRset décrites dans la [RFC2181].

Fichier maître *(Master file)* : les "fichiers maîtres sont des fichiers de texte qui contiennent des RR en forme de texte. Comme le contenu d'une zone peut être exprimé sous la forme d'une liste de RR, un fichier maître est très souvent utilisé pour définir une zone, bien qu'il puisse être utilisé pour faire la liste du contenu d'une antémémoire." (Cité de la [RFC1035], Section 5). Les fichiers maîtres sont parfois appelés "fichiers de zone".

Format de présentation : format de texte utilisé dans les fichiers maîtres. Ce format est montré mais non défini formellement dans la [RFC1034] ou la [RFC1035]. Le terme "format de présentation" est apparu pour la première fois dans la [RFC4034].

EDNS : mécanismes d'extension du DNS, défini dans la [RFC6891]. Parfois appelé "EDNS0" ou "EDNS(0)" pour indiquer le numéro de version. EDNS permet aux clients et serveurs DNS de spécifier des tailles de message supérieures à la limite originelle de 512 octets, pour étendre l'espace de code de réponse et pour porter des options supplémentaires qui affectent le traitement d'une interrogation du DNS.

OPT : pseudo-RR (parfois appelé un "méta-RR") qui n'est utilisé que pour contenir des informations de contrôle relevant de la séquence de question-réponse d'une transaction spécifique. (Définition paraphrasée de la [RFC6891], paragraphe 6.1.1.) Elle est utilisée par EDNS.

Propriétaire *(Owner)* : "Le nom de domaine où se trouve le RR." (Cité de la [RFC1034], paragraphe 3.6). Le terme "nom de propriétaire" apparaît souvent.

Noms de champ SOA : les documents du DNS, incluant les définitions données ici se réfèrent souvent aux champs dans les RDATA d'un enregistrement de ressource SOA par un nom de champ. "SOA" signifie "début de zone d'autorité" *(start of a zone of authority)*. Ces champs sont définis au paragraphe 3.3.13 de la [RFC1035]. Les noms (dans l'ordre de leur apparition dans le SOA des RDATA) sont MNAME, RNAME, SERIAL, REFRESH, RETRY, EXPIRE, et MINIMUM. Noter que la signification du champ MINIMUM est mise à jour par la Section 4 de la [RFC2308] ; la nouvelle définition est que le champ MINIMUM est seulement "le TTL à utiliser pour les réponses négatives". Le présent document tend à utiliser les noms de champs plutôt que les termes qui décrivent les champs.

TTL : la "durée de vie" maximum d'un enregistrement de ressource. "Une valeur de TTL est un un entier non signé, d'une valeur minimum de 0, et d'une valeur maximum de 2 147 483 647. C'est-à-dire un maximum de 2^31 - 1. À l'émission, cette valeur doit être codée sur les 31 bits de moindre poids du champ TTL de 32 bits, avec le bit de poids fort, ou signe, réglé à zéro." (Cité de la [RFC2181], Section 8). (Noter que la [RFC1035] déclare par erreur que c'est un entier signé ; cela a été corrigé dans la [RFC2181].)

Le TTL "spécifie l'intervalle de temps pendant lequel l'enregistrement de ressource peut être conservée en antémémoire avant que la source des informations doive être consultée à nouveau." (Cité de la [RFC1035], paragraphe 3.2.1). Le paragraphe 4.1.3 du même document déclare : "l'intervalle de temps (en secondes) pendant lequel l'enregistremet de ressource peut être conservé en antémémoire avant qu'elle doive être supprimée". En dépit du fait qu'il est défini pour un enregistrement de ressource, il est exigé du TTL de tous les enregistrements de ressource d'un RRset qu'il soit le même pour tous ([RFC2181], paragraphe 5.2).

La raison pour laquelle le TTL est la durée de vie maximum est que l'opérateur de l'antémémoire pourrait décider d'abréger le temps de vie pour des raisons opérationnelles, comme si il y a une politique d'interdire des valeurs de TTL supérieures à un certain nombre. Certains serveurs sont connus pour ignorer le TTL sur certains RRsets (comme lorsque les données

d'autorité ont un TTL très court) même si c'est contraire à l'avis de la RFC 1035. Un RRset peut être purgé de l'antémémoire avant la fin de l'intervalle de TTL, auquel cas, la valeur du TTL devient inconnue parce que le RRset auquel il était associé n'existe plus.

Il y a aussi le concept d'un "TTL par défaut" pour une zone, qui peut être un paramètre de configuration dans le logiciel du serveur. Ceci est souvent exprimé par une valeur par défaut pour le serveur entier, et une valeur par défaut pour une zone qui utilise la directive $TTL dans un fichier de zone. La directive $TTL a été ajoutée au format de fichier maître par la [RFC2308].

Indépendant de la classe : type d'enregistrement de ressource dont la syntaxe et la sémantique sont les mêmes pour toutes les classes du DNS. Un type d'enregistrement de ressource qui n'est pas indépendant de la classe a des significations différentes selon la classe DNS de l'enregistrement, ou la signification est indéfinie pour certaines classes. La plupart des types d'enregistrements de ressource sont définis pour la classe 1 (IN, Internet), mais beaucoup sont indéfinis pour les autres classes.

Enregistrement d'adresse *(Address record)* : enregistrements dont le type est A ou AAAA. La [RFC2181] les définit de façon informelle comme "(A, AAAA, etc)". Noter que de nouveaux types d'enregistrements d'adresse pourraient être définis à l'avenir.

6. Serveurs et clients DNS

Cette section définit les termes utilisés pour les systèmes qui agissent comme des clients du DNS, des serveurs du DNS, ou les deux. Dans les RFC du passé, les serveurs DNS sont parfois appelés "serveurs de noms ", ou juste "serveurs". Il n'y a pas de définition formelle d'un "serveur DNS", mais les RFC supposent généralement que c'est un serveur Internet qui écoute les interrogations et envoie les réponses en utilisant le protocole DNS défini dans la [RFC1035] et ses successeurs.

Il est important de noter que les termes "serveur DNS" et "serveur de noms" exigent un contexte afin de comprendre les services qui sont fournis. Les serveurs d'autorité et les résolveurs récurrents sont souvnet appelés "serveurs DNS" et "serveurs de noms" même si ils servent des rôles différents (mais peuvent faire partie du même paquetage logiciel).

Pour la terminologie spécifique du système de serveur racine du DNS public, voir [RSSAC026]. Ce document définit des termes comme "serveur racine", "opérateur de serveur racine", et des termes qui sont spécifique de la façon dont la zone racine du DNS public est desservie.

Résolveur : programme "qui extrait des informations des serveurs de noms en réponse aux demandes du client." (Cité de la [RFC1034], paragraphe 2.4). Un résolveur effectue des interrogations sur un nom, type, et classe, et reçoit des réponses. La fonction logique est appelée "résolution". En pratique, le terme se réfère généralement à un type spécifique de résolveur (dont certains sont définis ci-dessous) et la compréhension de l'usage du terme dépend de la compréhension du contexte.

Un terme en rapport est "résoudre", qui n'est pas formellement défini dans la [RFC1034] ou la [RFC1035]. Une définition déduite pourrait être "poser une question qui consiste en un nom de domaine, sa classe, et son type, et à recevoir quelque sorte de réponse". de même, une définition déduite de "résolution" pourrait être "la réponse reçue pour résoudre".

Résolveur d'extrémité *(stub resolver)* : résolveur qui ne peut pas effectuer toute la résolution lui-même. Les résolveurs d'extrémité dépendent généralement d'un résolveur récurrent pour entreprendre la fonction de résolution réelle. Les résolveurs d'extrémité sont discutés mais jamais bien définis au paragraphe 5.3.1 de la [RFC1034]. Ils sont pleinement définis au paragraphe 6.1.3.1 de la [RFC1123].

Mode itératif *(Iterative mode)* : mode de résolution d'un serveur qui reçoit des interrogations de DNS et répond par un point de référence à un autre serveur. Le paragraphe 2.3 de la [RFC1034] décrit cela comme "Le serveur renvoie le client à un autre serveur et laisse le client poursuivre l'interrogation". Un résolveur qui travaille en mode itératif est parfois appelé un "résolveur itératif". Voir aussi "résolution itérative" plus loin.

Mode récurrent *(Recursive mode)* : mode de résolution d'un serveur qui reçoit des interrogations du DNS et soit répond à ces interrogations à partir d'une antémémoire locale, soit envoie les interrogations à d'autres serveurs afin d'obtenir les réponses finales aux interrogations d'origine. Le paragraphe 2.3 de la [RFC1034] décrit cela comme "le premier serveur poursuit l'interrogation pour le client sur un autre serveur". Le paragraphe 4.3.1 de la [RFC1034] dit : "en mode [récurrent] le serveur de noms agit dans le rôle d'un résolveur et retourne soit une erreur, soit la réponse, mais jamais de points de référence". Le même paragraphe dit aussi : "Le mode récurrent se produit lorsque une interrogation avec RD établi arrive

au serveur qui veut fournir le service récurrent ; le client peut vérifier que le mode récurrent a été utilisé en vérifiant que RA et RD sont tous deux établis dans la réponse".

Un serveur qui fonctionne en mode récurrent peut être vu comme ayant un côté serveur de noms (qui est ce qui répond à l'interrogation) et un côté résolveur (qui effectue la fonction de résolution). Les systèmes qui fonctionnenent dans ce mode sont couramment appelés "serveurs récurrents". Parfois ils sont appelés "résolveurs récurrents". En pratique, il n'est pas possible de savoir à l'avance si le serveur qu'on interroge va aussi effectuer la récurrence ; les deux termes peuvent être utilisés de façon interchangeable.

Résolveur récurrent *(Recursive resolver)* : résolveur qui agit en mode récurrent. En général, un résolveur récurrent est supposé mettre en antémémoire les réponses qu'il reçoit (ce qui en ferait un résolveur de plein exercice) mais certains résolveurs récurrents peuvent ne pas mettre en antémémoire. La [RFC4697] a essayé de différencier résolveur récurrent et itératif.

Interrogation récurrente *(Recursive query)* : interrogation dont le bit Récurrence désirée (RD, *Recursion Desired*) est réglé à 1 dans l'en-tête (voir le paragraphe 4.1.1 de la [RFC1035]). Si le service de récurrence est disponible et est demandé par le bit RD dans l'interrogation, le serveur utilise son résolveur pour répondre à l'interrogation (voir le paragaphe 4.3.2 de la [RFC1034]).

Interrogation non récurrente *(Non-recursive query)* : interrogation avec le bit Récurrence désirée (RD) réglé à 0 dans l'en-tête. Un serveur peut répondre aux interrogations non récurrentes en utilisant seulement des informations locales : la réponse contient une erreur, la réponse, ou un point de référence à un autre serveur "plus proche" de la réponse (voir le paragraphe 4.3.1 de la [RFC1034].)

Résolution itérative : un serveur de noms peut recevoir une interrogation à laquelle seul un autre serveur peut répondre. Les deux approches générales pour traiter ce problème sont la résolution "récurrente", dans laquelle le premier serveur poursuit l'interrogation au nom du client sur un autre serveur, et la résolution "itérative", dans laquelle le serveur renvoie le client sur un autre serveur et laisse le client y poursuivre l'interrogation (voir le paragraphe 2.3 de la [RFC1034]).
Dans la résolution itérative, le client fait de façon répétée des interrogations non récurrentes et suit les points de référence et/ou alias. L'algorithme de résolution itérative est décrit au paragraphe 5.3.3 de la [RFC1034].

Plein résolveur *(Full resolver)* : ce terme est utilisé dans la [RFC1035], mais n'y est pas défini. La RFC 1123 définit un "résolveur de service plein" qui peut être ou non ce qui est entendu par "plein résolveur" dans la [RFC1035]. Ce terme n'est vraiment défini dans aucune RFC.

Résolveur de service plein *(Full-service resolver)* : le paragraphe 6.1.3.1 de la [RFC1123] définit ce terme comme signifiant un résolveur qui agit en mode récurrent avec une antémémoire (et satisfait à d'autres exigences).

Amorçage *(Priming)* : "action de trouver la liste des serveurs racines à partir d'une configuration qui fait la liste de certaines ou toutes les adresses IP supposées de certains de ces serveurs racines, ou de tous". (Cité de la [RFC8109], Section 2) Afin de fonctionner en mode récurrent, un résolveur a besoin de connaître l'adresse d'au moins un serveur racine. L'amorçage est le plus souvent fait à partir d'un réglage de configuration qui contient une liste des serveurs d'autorité pour la zone racine.

Conseils de racine *(Root hints)* : "les opérateurs qui gèrent un résolveur récurrent du DNS ont normalement besoin de configurer un "fichier de conseils de racine". Ce fichier contient les noms et adresses IP des serveurs de noms d'autorité pour la zone racine, afin que le logiciel puisse amorcer le processus de résolution du DNS. Pour de nombreux éléments de logicel, cette liste est incorporée dans le logiciel". (Cité de [IANA_RootFiles]) Ce fichier est souvent utilisé dans l'amorçage.

Mise en antémémoire négative *(Negative caching)* : "La mémorisation de la connaissance que quelque chose n'existe pas, ne peut pas donner ou ne donne pas de réponse". (Cité de la [RFC2308], Section 1)

Serveur d'autorité *(Authoritative server)* : "Serveur qui connaît le contenu d'une zone du DNS à partir de connaissances locales, et peut donc répondre aux interrogations sur cette zone sans avoir besoin d'interroger d'autres serveurs". (Cité de la [RFC2182], Section 2). Un serveur d'autorité est nommé dans l'enregistrement NS ("serveur de noms") d'une zone. C'est un système qui répond aux interrogations au DNS avec les informations sur les zones pour lesquelles il a été configuré à répondre avec le fanion AA dans l'en-tête de réponse réglé à 1. C'est un serveur qui a autorité sur une ou plusieurs zones du DNS. Noter qu'il est possible à un serveur d'autorité de répondre à une interrogation sans que la zone parente délègue l'autorité à ce serveur. Les serveurs d'autorité fournissent aussi des "points de référence", généralement aux zones filles auxquelles ils donnent délégation ; ces points de référence ont le bit AA réglé à 0 et viennent avec les données de point de référence dans les sections Autorité et (si nécessaire) Additionnelle.

Serveur seulement d'autorité *(Authoritative-only server)* : serveur de noms qui ne sert que pour les données d'autorité et ignore les demandes en récurrence. Il ne va "normalement pas générer d'interrogations de lui-même. Il répond plutôt aux interrogations non récurrentes provenant de résolveurs itératifs qui cherchent des informations dans les zones qu'il dessert". (Cité de la [RFC4697], paragraphe 2.4). Dans ce cas, "ignore les demandes en récurrence" signifie "répond aux demandes en récurrence avec des réponses indiquant que la récurrence n'a pas été effectuée".

Transfert de zone : acte d'un client qui demande une copie d'une zone et d'un serveur d'autorité qui envoie les informations nécessaires (voir à la Section 7 la description des zones). Il y a deux façons standard courantes pour faire des transferts de zone : le mécanisme AXFR ("Transfert d'autorité") pour copier toute la zone (décrite dans la [RFC5936], et le mécanisme IXFR ("Transfert incrémentaire") pour copier seulement des parties de la zone qui ont changé (décrit dans la [RFC1995]). De nombreux systèmes utilisent des méthodes non standard pour des transferts de zone en dehors du protocole DNS.

Serveur esclave : voir "Serveur secondaire".

Serveur secondaire : "serveur d'autorité qui utilise un transfert de zone pour restituer la zone". (Cité de la [RFC1996], paragraphe 2.1). Les serveurs secondaires sont aussi discutés dans la [RFC1034]. La [RFC2182] décrit les serveurs secondaires plus en détail. Bien que les premières RFC sur le DNS comme la [RFC1996] se rèfèrent à cela comme à un "esclave", l'usage courant commun est passé à l'appellation de "secondaire".

Serveur maître *(Master server)* : voir "Serveur principal".

Serveur principal *(Primary server)* : "tout serveur d'autorité configuré pour être la source de transfert de zone pour un ou plusieurs serveurs [secondaires]". (Cité de la [RFC1996], paragraphe 2.1). Ou, plus précisémentt, la [RFC2136] l'appelle un "serveur d'autorité configuré pour être la source des données AXFR ou IXFR pour un ou plusieurs serveurs [secondaires]". Les serveurs principaux sont aussi discutés dans la [RFC1034]. Bien que les premières RFC sur le DNS comme la [RFC1996] se rèfèrent à cela comme à un "maître", l'usage courant commun est passé à l'appellation de "principal".

Maître principal *(Primary master)* : "Le maître principal est nommé dans le champ MNAME du SOA de la zone et facultativement par un RR NS". (Cité de la [RFC1996], paragraphe 2.1). La [RFC2136] définit un "maître principal" comme un "serveur maître à la racine du graphe de dépendance AXFR/IXFR. Le maître principal est nommé dans le champ MNAME du SOA de la zone et facultativement par un RR NS. Il y a par définition un seul serveur maître principal par zone."
L'idée de maître principal n'est utilisée que dans les [RFC1996] et [RFC2136]. Une interprétation moderne du terme "maître prncipal" est que c'est un serveur qui est à la fois d'autorité pour une zone et qui obtient ses mises à jour de la zone de la configuration (comme un fichier maître) ou de transactions UPDATE.

Serveur furtif *(Stealth server)* : c'est comme "un serveur esclave sauf qu'il ne figure pas sur la liste dans un RR NS pour la zone". (Cité de la [RFC1996], paragraphe 2.1).

Maître caché *(Hidden master)* : serveur furtif qui est un serveur principal pour les transferts de zone. "Dans cet arrangement, le serveur de noms maître qui traite les mises à jour est indisponible pour les hôtes généraux de l'Internet ; il ne figure pas sur la liste dans le RRset NS". (Cité de la [RFC6781], paragraphe 3.4.3). Une RFC précédente, [RFC4641], disait que le nom du maître caché "apparaît dans le champ MNAME de SOA des RR", bien que dans certaines mises en œuvre, le nom n'apparaisse pas du tout dans le DNS public. Un maître caché peut aussi être un serveur secondaire pour la zone elle-même.

Transmission *(Forwarding)* : processus par lequel un serveur envoie une interrogation au DNS avec le bit RD réglé à 1 pour qu'un autre serveur résolve cette interrogation. La transmission est une fonction d'un résolveur DNS ; elle est différente d'un simple relais aveugle des interrogations.
La [RFC5625] ne donne pas une définition spécifique pour "transmission", mais décrit en détail quelles caractéristiques doit prendre en charge un système qui transmet. Les systèmes qui transmettent sont parfois appelés des "mandataires DNS", mais ce terme n'a pas encore été défini (même dans la [RFC5625]).

Transmetteur *(Forwarder)* : la Section 1 de la [RFC2308] décrit un transmetteur comme "un serveur de noms utilisé pour résoudre des interrogations au lieu d'utiliser directement la chaîne des serveurs de noms d'autorité". La [RFC2308] dit de plus que "le transmetteur a normalement un meilleur accès à l'internet, ou possède une plus grosse antémémoire qui peut être partagée entre de nombreux résolveurs". Cette définition paraît suggérer que les transmetteurs n'interrogent normalement que les serveurs d'autorité. Dans l'usage courant, cependant, les transmetteurs se tiennent souvent entre les résolveurs d'extrémité et les serveurs récurrents. La [RFC2308] est silencieuse sur la question de savoir si un transmetteur est seulement itératif ou si il peut être un résolveur de service plein.

Résolveur de mise en œuvre de politique *(Policy-implementing resolver)* : résolveur agissant en mode récurrent qui change

certaines des réponses qu'il retourne sur la base de critères de politique, comme d'empêcher l'accès aux sites malveillants ou de contenu discutable. En général, un résolveur d'extrémité n'a pas d'élément pour savoir si les résolveurs en amont mettent en œuvre une telle politique ou, s'il en a, sur la politique exacte sur laquelle des changements seront faits. Dans certains cas, l'utilisateur du résolveur d'extrémité a choisi le résolveur de mise en œuvre de politique avec l'intention explicite de l'utiliser pour mettre en œuvre les politiques. Dans d'autres cas, les politiques sont imposées sans que l'utilisateur du résolveur d'extrémité en soit informé.

Résolveur ouvert *(Open resolver)* : résolveur de service plein qui accepte et traite les interrogations provenant de tout (ou presque tout) client. C'est parfois appelé aussi un "résolveur public", bien que le terme "résolveur public" soit utilisé plutôt avec des résolveurs ouverts qui sont destinés à être ouverts, par opposition à la vaste majorité des résolveurs ouverts qui sont probablement mal configurés pour être ouverts. Les résolveurs ouverts sont discutés dans la [RFC5358].

DNS partagé *(Split DNS)* : les termes "DNS partagé" et "DNS à horizon partagé" ont longtemps été utilisés dans la communauté du DNS sans définition formelle. En général, ils se réfèrent à des situations dans lesquelles les serveurs DNS qui sont d'autorité pour un ensemble particulier de domaines fournissent des réponses partiellement ou complètement différentes dans ces domaines selon la source de l'interrogation. Cela a pour effct qu'un nom de domaine qui est en principe unique au monde a néanmoins des significations différentes pour des utilisateurs différents du réseau. Cela peut parfois être le résultat d'une configuration de "vue", décrite ci-dessous. Le paragraphe 3.8 de la [RFC2775] donne une définition relative qui est trop spécifique pour être d'utilité générale.

Vue : une configuration d'un serveur DNS qui lui permet de fournir des réponses différentes selon les attributs de l'interrogation, comme pour le "DNS partagé". Normalement, les vues diffèrent par l'adresse IP de source d'une interrogation, mais peuvent aussi se fonder sur l'adresse IP de destination, le type d'interrogation (comme AXFR) si il est récurrent, et ainsi de suite. Les vues sont souvent utilisées pour fournir plus de noms ou des adresses différentes aux interrogations provenant "de l'intérieur" d'un réseau protégé qu'à celles provenant de "l'extérieur" de ce réseau. Les vues ne sont pas une partie normalisée du DNS, mais sont largement mises en œuvre dans le logiciel de serveur.

DNS passif : mécanisme pour collecter des données du DNS en mémorisant les réponses du DNS provenant des serveurs de noms. Certains de ces systèmes collectent aussi les interrogations au DNS associées aux réponses, bien que le faire soulève des problèmes de confidentialité. Les bases de données de DNS passif peuvent être utilisées pour répondre à des questions d'historique sur les zones DNS comme quelles valeurs étaient présentes à un instant donné dans le passé, ou quand un nom a été repéré pour la première fois. Les bases de données de DNS passif permettent des recherches sur les enregistrements mémorisés sur des clés autres que les seuls nom et type, comme "trouver tous les noms qui ont des enregistrements A d'une certaine valeur".

Envoi à la cantonade *(Anycast)* : "pratique consistant à rendre disponible l'adresse d'un service particulier dans plusieurs localisations autonomes distinctes, telle que les datagrammes envoyés sont acheminés à une de ces diverses localisations disponibles". (Cité de la [RFC4786], Section 2). Voir dans la [RFC4786] les détails sur l'envoi à la cantonade et autres termes spécifiques de son utilisation.

Instance : "quand l'acheminement en envoi à la cantonade est utilisé pour permettre à plus d'un serveur d'avoir la même adresse IP, on se réfère généralement à chacun de ces serveurs comme à une "instance". Cela amène à dire : "une instance d'un serveur, comme un serveur racine, est souvent appelée une "instance d'envoi à la cantonade"." (Cité d'après [RSSAC026]).

Serveur DNS à capacité de confidentialité *(Privacy-enabling DNS server)* : "serveur DNS qui met en œuvre le DNS sur TLS [RFC7858] et peut facultativement mettre en œuvre le DNS sur DTLS [RFC8094]." (Cité d'après la [RFC8310], Section 2). D'autres types de serveurs DNS peuvent aussi être considérés comme à capacité de confidencialité, comme ceux qui mettent en œuvre le DNS sur HTTPS [RFC8484].

7. Zones

Cette section définit les termes qui sont utilisés lorsque on parle de zones qui sont desservies ou restituées.

Zone : "informations d'autorité qui sont organisée en unités appellées ZONES, et ces zones peuvent être automatiquement distribuées entre les serveurs de noms qui fournissent un service redondant pour les données dans une zone." (Cité de la [RFC1034], paragraphe 2.4)

Enfant *(Child)* : "entité qui a la délégation du domaine de la part du parent." (Cité de la [RFC7344], paragraphe 1.1)

Parent : "domaine dans lequel l'enfant est enregistré." (Cité de la [RFC7344], paragraphe 1.1). Antérieurement, "serveur de noms parent" était défini dans la [RFC0882] comme "le serveur de noms qui a autorité sur l'endroit de l'espace des noms de domaines qui va contenir le nouveau domaine". (Noter que la [RFC0882] a été rendue obsolète par les [RFC1034] et [RFC1035].) La [RFC819] a aussi une description des relations entre parents et enfants.

Origine :

Il y a deux utilisations différentes pour ce terme :

(a) "Le nom de domaine qui apparaît comme sommet d'une zone (juste en dessous de la coupure qui sépare la zone de son parent)... Le nom de la zone est le même que le nom du domaine à l'origine de la zone." (Cité de la [RFC2181], Section 6). Aujourd'hui, ce sens de "origine" et "apex" (défini ci-dessous) sont souvent utilisés de façon interchangeable.

(b) Le nom de domaine au sein duquel un certain nom de domaine relatif apparaît dans les fichiers de zone. Généralement vu dans le contexte de "$ORIGIN", qui est une entrée de contrôle définie dans la [RFC1035], paragraphe 5.1, comme partie du format de fichier maître. Par exemple, si la $ORIGIN est réglée à "exemple.org.", une ligne de fichier maître pour "www" est en fait une entrée pour "www.exemple.org.".

Apex : point de l'arborescence à un propriétaire d'un SOA et du RRset NS d'autorité correspondant. C'est aussi appelé "apex de zone". La [RFC4033] le définit comme "le nom du côté enfant de la coupure de zone". Un "apex" peut utilement être imaginé comme une description théorique en termes de données d'une structur d'arborescencee, et "origine" est le nom du même concept quand il est mis en œuvre dans les fichiers de zone. La distinction n'est cependant pas toujours conservée dans l'usage courant, et on trouvera des cas d'utilisation qui entrent subtilement en conflit avec cette définition. La [RFC1034] utilise le terme de "nœud supérieur de la zone" comme synonyme de "apex", mais ce terme n'est pas largement utilisé. Aujourd'hui, le premier sens de "origine" (ci-dessus) et de "apex" sont souvent utilisés de façon interchangeable.

Coupure de zone *(Zone cut)* : point de délimitation entre deux zones où l'origine de l'une des zones est l'enfant de l'autre zone. Les "zones sont délimitées par des "coupures de zone". Chaque coupure de zone sépare une zone "fille" (en dessous de la coupure) d'une zone "'parente" (au dessus de la coupure)." (Cité de la [RFC2181], Section 6 ; noter que c'est simplement une définition apparente.) Le paragraphe 4.2 de la [RFC1034] utilise "coupures" à la place de "coupures de zone".

Délégation : processus par lequel une zone séparée est créée dans l'espace de noms en dessous de l'apex d'un certain domaine. Une délégation survient quand un RRset NS est ajouté à la zone parente pour l'origine de l'enfant. Une délégation apparaît naturellement à une coupure de zone. Le terme est aussi couramment un nom : la nouvelle zone créée par l'acte de délégation.

Données d'autorité *(Authoritative data)* : "Tous les RR rattachés à tous les nœuds depuis le nœud au sommet de la zone jusqu'aux nœuds feuilles ou nœuds au dessus de coupures autour du fond de la zone." (Cité de la [RFC1034], paragraphe 4.2.1). Noter que cette définition pourrait par inadvertence faire apparaître tous les enregistrements NS qui apparaissent dans la zone comme étant inclus, même ceux qui ne seraient pas vraiment d'autorité parce qu'ils sont identiques aux RR NS d'en dessous de la coupure de zone. Cela révèle l'ambiguïté de la notion de données d'autorité, parce que les enregistrements NS du côté parent ont autorité pour indiquer la délégation, même si ils ne sont pas eux-mêmes des données d'autorité. La [RFC4033], à sa Section 2, définit un "RRset d'autorité", qui se rapporte aux données d'autorité mais a une définition plus précise.

Délégation boîteuse *(Lame delegation)* : "il existe une délégation boîteuse [sic] quand un serveur de noms a reçu une délégation de responsabilité pour la fourniture du service de noms pour une zone (via des enregistrements NS) mais qu'il n'effectue pas le service de noms pour cette zone (généralement parce qu'il n'est pas constitué en serveur principal ou secondaire pour la zone)". (Cité de la [RFC1912], paragraphe 2.8). Une autre définition est qu'une délégation boîteuse"...se produit quand un serveur de noms figure sur la liste des enregistrements NS pour un certain domaine alors qu'en fait il n'est pas un serveur pour ce domaine. Les interrogations sont donc envoyées aux mauvais serveurs, qui ne savent rien (au moins pas ce qui est attendu) du domaine interrogé. De plus, parfois ces hôtes (si ils existent !) ne fonctionnent même pas comme serveurs de noms". (Cité de la [RFC1713], paragraphe 2.3)

Enregistrements glu *(Glue records)* : "...[enregistrements de ressources] qui ne font pas partie des données d'autorité [de la zone], et sont des RR d'adresses pour les serveurs [de noms dans les sous zones]. Ces RR ne sont nécessaires que si le nom du serveur de noms est "en dessous" de la coupure, et ne sont utilisés qu'au titre d'une réponse de point de référence". Sans glu "on devrait faire face à une situation où les RR NS nous diraient qu'afin de savoir l'adresse d'un serveur de noms, on devrait contacter le serveur en utilisant l'adresse qu'on souhaite avoir". (Cité de la [RFC1034], paragraphe 4.2.1). Une définition ultérieure est que les enregistrements glu "incluent tous les enregistrements d'un fichier zone qui ne font pas à proprement parler partie de cette zone, incluant les enregistrements de serveur de noms des sous zones déléguées (enregistrements NS) les enregistrements d'adresses qui accompagnent ces enregistrements NS (A, AAAA, etc), et toutes

les autres données errantes qui pourraient apparaître". (Cité de la [RFC2181], paragraphe 5.4.1). Bien que glu soit parfois utilisé aujourd'hui avec une définition plus large, le contexte environnant de la définition de la [RFC2181] suggère qu'elle est destinée à s'appliquer à l'usage de glu au sein du document lui-même et pas nécessairement au delà.

Sous la dépendance de *(Bailiwick)* : "Sous la dépendance de" est un modificateur pour décrire un serveur de noms dont le nom est soit un sous domaine de, ou (rarement) le même que l'origine de la zone qui contient la délégation au serveur de noms. Les noms de serveurs sous la dépendance d'un autre peuvent avoir des enregistrements glu dans leur zone parente (en utilisant la première des définitions de "enregistrements glu" ci-dessus). (Le terme de "bailiwick" *(baillage)* signifie le district ou territoire où un bailli ou policier exerce sa juridiction.)
Les noms "sous la dépendance de "sont divisés en deux types de noms pour les serveurs de noms : les noms "dans le domaine" et les noms de "domaine jumeau".

* dans le domaine : modificateur pour décrire un serveur de noms dont le nom est subordonné à, ou (rarement) le même que le nom de propriétaire des enregistrements de ressource NS. Un nom de serveur de noms dans le domaine a besoin d'avoir des enregistrements glu sinon la résolution de noms va échouer. Par exemple, une délégation pour "enfant.exemple.com" peut avoir un nom de serveur de noms "dans le domaine" de "ns.enfant.exemple.com".
* domaine jumeau : un nom de serveur de noms qui est subordonné à, ou a (rarement) le même nom que l'origine de zone et n'est pas subordonné à ou a le même nom que le nom du propriétaire des enregistrements de ressource NS. Les enregistrements glu pour les domaines jumeaux sont permis, mais pas nécessairement. Par exemple, une délégation pour "enfant.exemple.com" dans la zone "exemple.com" peut avoir le nom de serveur de noms jumeau de "ns.unautre.exemple.com".

"Hors dépendance" *(Out-of-bailiwick)* est le contraire de "sous la dépendance". C'est un modificateur pour décrire un serveur de noms dont le nom n'est pas subordonné à, ou est le même que, celui de l'origine de zone. Les enregistrements glu pour les serveurs de noms hors de dépendance sont sans objet. Le tableau suivant montre des exemples de types de délégation.

Délégation	Parent	Nom de serveur de noms	Type
com	.	a.gtld-servers.net	sous dépendance / domaine jumeau
net	.	a.gtld-servers.net	sous dépendance / dans le domaine
example.org	org	ns.example.org	sous dépendance / dans le domaine
example.org	org	ns.ietf.org	sous dépendance / domaine jumeau
example.org	org	ns.example.com	hors dépendance
example.jp	jp	ns.example.jp	sous dépendance / dans le domaine
example.jp	jp	ns.example.ne.jp	sous dépendance / domaine jumeau
example.jp	jp	ns.example.com	hors dépendance

Zone racine *(Root zone)* : zone d'une arborescence fondée sur le DNS dont l'apex est l'étiquette de longueur zéro. Aussi appelée parfois "racine du DNS".

Vides non terminaux (ENT, *Empty non-terminal*) : "Noms de domaines qui ne possèdent pas d'enregistrement de ressource mais ont des sous domaines qui en ont". (Cité de la [RFC4592], paragraphe 2.2.2). Un exemple typique est dans des enregistrements SRV : dans le nom "_sip._tcp.example.com", il est probable que "_tcp.example.com" n'a pas de RRset, mais que "_sip._tcp.example.com" a (au moins) un RRset SRV.

Zone centrée sur la délégation *(Delegation-centric zone)* : zone qui consiste principalement en délégations à des zones filles. Ce terme est utilisé par opposition à une zone qui pourrait avoir des délégations à des zones filles mais a aussi de nombreux enregistrements de ressources de données pour la zone elle-même et/ou pour ses zones filles. Le terme est utilisé dans les [RFC4956] et [RFC5155], mais n'est pas défini dans ces documents.

Nom occlus *(Occluded name)* : "L'ajout d'un point de délégation via une mise à jour dynamique va plonger tous les noms de domaines subordonnés dans les limbes, faisant toujours partie de la zone mais non disponibles au processus de recherche. L'ajout d'un enregistrement de ressource DNAME a le même impact. Les noms subordonnés sont dits être 'occlus' . (Cité de la [RFC5936], paragraphe 3.5)

DNS à flux rapide *(Fast flux DNS)* : cela "se produit quand un domaine [se trouve] dans le DNS qui utilise des enregistrements A sur plusieurs adresses IP, dont chacune a une valeur de durée de vie (TTL *Time-to-Live*) très courte qui lui est associée. Cela signifie que le domaine se résout en diverses adresses IP sur une période brève". (Cité de la [RFC6561], paragraphe 1.1.5, avec une faute de frappe corrigée). En plus d'avoir des utilisations légitimes, le DNS à flux rapides peut être utilisé pour délivrer des logiciels malveillants. Parce que les adresses changent si rapidement, il est difficile de s'assurer de tous les hôtes. On devrait noter que la technique fonctionne aussi avec les enregistrements AAAA, mais une telle utilisation n'est pas fréquemment observée sur l'Internet à l'heure où nous écrivons.

DNS inverse, recherche inverse : "le processus de transposition d'une adresse en nom est généralement connu sous le nom de "recherche inverse", et les zones IN-ADDR.ARPA et IP6.ARPA sont dites prendre en charge le 'DNS inverse'". (Cité de la [RFC5855], Section 1)

Recherche vers l'avant *(Forward lookup)* : "Traduction de nom d'hôte en adresse". (Cité de la [RFC3493], Section 6)

arpa *(Address and Routing Parameter Area Domain)* : domaine de zone de paramètres d'adresse et d'acheminement. "Le domaine 'arpa' a été à l'origine établi au titre du déploiement initial du DNS, pour fournir un mécanisme de transition du Tableau des hôtes qui était utilisé dans l'ARPANET, ainsi que comme hébergement du domaine de transposition de IPv4 inverse. Durant les années 2000, l'abréviation a été renommée en 'zone de paramètres d'adresse et d'acheminement" dans l'espoir de réduire la confusion avec l'ancien nom du réseau". (Cité de la [RFC3172], Section 2). .arpa est un "domaine d'infrastructure", un domaine dont le "rôle est de prendre en charge l'infrastructure de fonctionnement de l'Internet". (Cité de la [RFC3172], Section 2). Voir dans la [RFC3172] l'historique de ce nom.

Nom de service : "Les noms de service sont la clé unique dans le registre de noms de service et des numéros de protocoles de transport. Ce nom symbolique unique pour un service peut aussi être utilisé à d'autres fins, comme dans les enregistrements SRV du DNS". (Cité de la [RFC6335], Section 5)

8. Caractères génériques

Caractère générique *(Wildcard)* : La [RFC1034] a défini le "caractère générique", mais d'une façon qui s'est révélée plonger les développeurs dans la confusion. Pour une large discussion sur les caractères génériques, incluant de plus claires définitions, voir la [RFC4592]. Un traitement particulier est réservé aux RR avec des noms de propriétaire commençant par l'étiquette "*". "De tels RR sont appelés des 'RR génériques'. Les RR génériques peuvent être vus comme des instructions pour synthéstiser les RR". (Cité de la [RFC1034], paragraphe 4.3.3)

Étiquette astérisque : "Le premier octet est le type d'étiquette normal et sa longueur est une étiquette d'un octet, et le second octet est la représentation en ASCII [RFC0020] du caractère '*'. Un nom descriptif d'une étiquette étant égal à cette valeur est une étiquette 'astérisque'". (Cité de la [RFC4592], paragraphe 2.1.1)

Nom de domaine générique *(Wildcard domain name)* : "Un nom de domaine générique' est défini comme ayant son étiquette initiale (c'est-à-dire, la plus à gauche ou de moindre poids) en format binaire : 0000 0001 0010 1010 (binaire) = 0x01 0x2a (hexadécimal)". (Cité de la [RFC4592], paragraphe 2.1.1). Le second octet dans cette étiquette est la représentation ASCII du caractère "*".

Englobeur le plus proche *(Closest encloser)* : "Le plus long ancêtre existant d'un nom". (Cité de la [RFC5155], paragraphe 1.3). Une définition antérieure est "Le nœud dans l'arboresecence de la zone des noms de domaines existants qui a le plus d'étiquettes correspondant au nom de l'interrogation (consécutivement, en comptant depuis d'étiquette racine). Chaque correrspondance est une "correspondance d'étiquette et l'ordre des étiquettes est le même". (Cité de la [RFC4592], paragraphe 3.3.1)

Plus proche englobeur démontrable *(Closest provable encloser)* : "plus long ancêtre d'un nom dont l'existence peut être prouvée. Noter que ceci n'est différent de l'englobeur le plus proche que dans une zone marqué du fanion Opt-Out". (Cité de la [RFC5155], paragraphe 1.3). La Section 10 en dit plus sur "opt-out".

Prochain nom plus proche *(Next closer name)* : "nom plus long d'une étiquette que le plus proche englobeur démontrable d'un nom." (Cité de la [RFC5155], paragraphe 1.3)

Source de synthèse : "la source de synthèse est définie dans le contexte d'un processus d'interrogation comme le nom de domaine à caractère générique qui descend immédiatement du plus proche englobeur, pourvu que ce nom de domaine à caractère générique existe. "Descendant immédiatement" signifie que la source de synthèse a un nom de la forme <étiquette astérisque>.<plus proche englobeur>". (Cité de la [RFC4592], paragraphe 3.3.1)

9. Modèle d'enregistrement

Registre : fonctionnement administratif d'une zone qui permet l'enregistrement des noms au sein de cette zone. Les gens

utilisent souvent le terme pour se référer uniquement aux organisations qui effectuent l'enregistrement dans de grandes zones fondées sur la délégation (comme les TLD) ; mais formellement, celui qui décide de quelles données vont dans une zone est le registre pour cette zone. Cette définition de "registre" est du point de vue du DNS ; pour certaines zones, la politique qui détermine ce qui peut aller dans la zone est décidé par les zones qui supervisent et non par l'opérateur du registre.

Registrant : organisation individuelle au nom de laquelle un nom est enregistré dans un zone par le registre. Dans de nombreuses zones, le registre et le registrant peuvent être la même entité, mais dans les TLD il ne le sont souvent pas.

Registraire : fournisseur de service qui agit comme intermédiaire entre registrants et registres. Tous les enregistrements n'exigent pas un registraire, bien qu'il soit courant d'avoir des registraires impliqués dans l'enregistrement dans les TLD.

Protocole de provisionnement extensible (EPP, *Extensible Provisioning Protocol*) : couramment utilisé pour la communication d'informations d'enregistrement entre registres et registraires. EPP est défini dans la [RFC5730].

WHOIS : protocole spécifié dans la [RFC3912], souvent utilisé pour interroger les bases de données de registres. Les données de WHOIS sont fréquemment utilisées pour associer les données d'enregistrement (comme les contacts de gestion de zone) aux noms de domaines. Le terme "données WHOIS" est souvent utilisé comme synonyme de base de données de registre, même si cette base de données peut être desservie par des protocoles différents, en particulier RDAP. Le protocole WHOIS est aussi utilisé avec les données de registre d'adresses IP.

Protocole d'accès aux données d'enregistrement (RDAP, *Registration Data Access Protocol*) : défini danns les [RFC7480], [RFC7481], [RFC7482], [RFC7483], [RFC7484], et [RFC7485]. Le protocole RDAP et le format des données sont destinés à remplacer WHOIS.

Opérateur DNS : entité chargé du fonctionnement des serveurs du DNS. Pour les serveurs d'autorité d'une zone, le registrant peut agir comme son propre opérateur DNS, leur registraire peut le faire en leur nom, ou ils peuvent utiliser un opérateur tiers. Pour certaines zones, la fonction de registre est effectuée par l'opérateur DNS plus d'autres entités qui décident des contenus permis de la zone.

Suffixe public : "domaine qui est sous le contrôle d'un registre public". (Cité de la [RFC6265], paragraphe 5.3). Une définition courante de ce terme est un domaine sous lequel des sous domaines peuvent être enregistrés par des tiers et sur lequel des mouchards HTTP (qui sont décrits de façon détaillée dans la [RFC6265]) ne devraient pas être établis. Il n'est pas indiqué dans un nom de domaine si c'est un suffice public ; cela ne peut être déterminé que par des moyens extérieurs. En fait, un domaine et un sous domaine de ce domaine peuvent tous deux être des suffixes publics.
Il n'y a rien d'inhérent dans un nom de domaine qui indique si il est un suffixe public. Une ressource pour identifier les suffixes publics est la liste des suffixes publics (PSL, *Public Suffix List*) tenue par Mozilla (http://publicsuffix.org/).
Par exemple, au moment de la publication du présent document, le domaine "com.au" figure sur la liste des suffixes publics dans la PSL. (Noter que cet exemple pourrait changer à l'avenir.)
Noter que le terme "suffixe public" peut prêter à controverse dans la communauté du DNS pour de nombreuses raisons, et il pourrait changer de façon significative à l'avenir. Un exemple de la difficulté d'appeler un domaine un suffixe public est que la désignation peut changer dans le temps avec les changements de la politique d'enregistrement pour la zone, comme cela a été le cas avec le TLD "uk" en 2014.

Subordonné et supérieur : ces termes sont introduits dans la [RFC5731] pour être utilisés dans le modèle d'enregistrement, mais n'y sont pas définis. Des exemples sont donnés à la place. "Par exemple, le nom de domaine 'exemple.com' a une relation de supérieur avec le nom d'hôte 'ns1.exemple.com'... Par exemple, l'hôte ns1.example1.com est un subordonné de l'hôte du domaine exemple1.com, mais il n'est pas un hôte subordonné du domaine exemple2.com". (Cité de la [RFC5731], paragraphe 1.1). Ces termes sont des façons strictes de se référer aux relations qui existent entre deux domaines où l'un est un sous domaine de l'autre.

10. DNSSEC général

La plupart des termes du DNSSEC sont définis dans les [RFC4033], [RFC4034], [RFC4035], et [RFC5155]. Les termes qui ont causé la confusion de la communauté du DNS sont repris ici.

À capacité DNSSEC et sans capacité DNSSEC *(DNSSEC-aware/unaware)* : Ces deux termes, qui sont utilisés dans certaines RFC, n'ont pas été formellement définis. Cependant, la Section 2 de la [RFC4033] définit de nombreux types de résolveurs et valideurs, incluant le "résolveur d'extrémité non valideur à capacité de sécurité", le "résolveur d'extrémité non valideur",

"le serveur de noms à capacité de sécurité", le "serveur de noms récurrent à capacité de sécurité", le "résolveur à capacité de sécurité", le "résolveur d'extrémité à capacité de sécurité", et le ""quelque chose" oublieux de la sécurité"". (Noter que le terme "résolveur validant", qui est utilisé en certains endroits de documents qui se rapportent au DSSEC, n'est pas non plus défini dans ces RFC, mais est défini ci-dessous.

Zone signée *(Signed zone)* : "zone dont les RRsets sont signés et qui contient des enregistrements DNSKEY, signature d'enregistrement de ressource (RRSIG, *Resource Record Signature*), Next Secure (NSEC), et (facultativement) DS construits de façon appropriée". (Cité de la [RFC4033], Section 2). On a noté dans d'autres contextes que la zone elle-même n'est pas réellement signée, mais tous les RRsets pertinents de la zone sont signés. Néanmoins, si une zone qui devrait être signée contient des RRsets qui ne sont pas signés (ou marqués "opted out") ces RRsets seront traités comme erronés, de sorte que la zone entière devrait être traitée d'une seule façon.
On notera aussi que, depuis la publication de la [RFC6840], les enregistrements NSEC ne sont plus exigés pour les zones signées : une zone signée peut inclure des enregistrements NSEC3 à la place. La [RFC7129] fournit des commentaires de fond supplémentaires et un contexte pour les mécanismes NSEC et NSEC3 utilisés par DNSSEC pour fournir des réponses authentifiées de déni d'existence. NSEC et NSEC3 sont décrits plus loin.

Zone non signée : La Section 2 de la [RFC4033] définit cela comme "une zone qui n'est pas signée". La Section 2 de la [RFC4035] définit cela comme une "zone qui ne comporte pas ces enregistrements [DNSKEY, signature d'enregistrement de ressource (RRSIG), Next Secure (NSEC), et (facultativement) DS construits de façon appropriée] conformément aux règles de cette section..." Il y a une note importante à la fin du paragraphe 5.2 de la [RFC4035] qui définit une situation supplémentaire dans laquelle une zone est considérée comme non signée : "Si le résolveur ne prend en charge aucun des algorithmes figurant sur la liste d'un RR DS authentifié, le résolveur ne sera alors pas capable de vérifier le chemin d'authentification jusqu'à la zone fille. Dans ce cas, le résolveur DEVRAIT traiter la zone fille comme non signée."

NSEC : "L'enregistrement NSEC permet à un résolveur à capacité de sécurité d'authentifier une réponse négative pour toute non existence de nom ou type avec les mêmes mécanismes qu'utilisés pour authentifier les autres réponses du DNS". (Cité de la [RFC4033], paragraphe 3.2). En bref, un enregistrement NSEC fournit un deni d'existence authentifié.
"L'enregistrement de ressource NSEC fait la liste de choses séparées : le prochain nom de propriétaire (dans l'ordre canonique de la zone) qui contient des données d'autorité ou un RRset NS de point de délégation, et l'ensemble des types de RR présents au nom de propriétaire du RR NSEC". (Cité de la Section 4 de la RFC 4034)

NSEC3 : comme l'enregistrement NSEC, l'enregistrement NSEC3 fournit aussi un déni d'existence authentifié ; cependant, les enregistrements NSEC3 atténuent l'énumération de zone et prennent en charge Opt-Out. Les enregistrements de ressource NSEC3 exigent des enregistrements de ressource NSEC3PARAM associés. Les enregistrements de ressource NSEC3 et NSEC3PARAM sont définis dans la [RFC5155].
Noter que la [RFC6840] dit que la [RFC5155] "est maintenant considérée comme une partie de la famille des documents sur la sécurité du DNS comme décrit à la Section 10 de la [RFC4033]". Cela signifie que certaines des définitions provenant des RFC antérieures qui parlent seulement des enregistrements NSEC devraient probablement être considérées comme parlant aussi bien de NSEC que de NSEC3.

Opt-out : "le fanion Opt-Out indique si ce RR NSEC3 peut couvrir des délégations non signées." (Cité de la [RFC5155], paragraphe 3.1.2.1). Opt-out vise les coûts élevés de la sécurisation d'une délégation à une zone non sûre. Quand on utilise Opt-Out, les noms qui sont une délégation non sûre (et un vide non terminal qui est seulement déduit de délégations non sûres) n'exigent pas un enregistrement NSEC3 ni son enregistrement RRSIG correspondant. Les enregistrements NSEC3 Opt-Out ne sont pas capables de prouver ou nier l'existence des délégations non sûres. (Adapté de la [RFC7129], paragraphe 5.1)

Délégation non sûre : "nom signé qui contient une délégation (RRset NS), mais n'a pas de RRset DS, ce qui signifie une délégation à une sous zone non signée." (Cité de la [RFC4956], Section 2).

Énumération de zone : "pratique de la découverte du contenu entier d'une zone via des interrogations successives." (Cité de la [RFC5155], paragraphe 1.3). C'est parfois appelé "parcours de zone". L'énumération de zone est différente de l'estimation du contenu d'une zone où celui qui estime utilise un grand dictionnaire d'étiquettes possibles et envoie des interrogations successives sur elles, ou confronte le contenu des enregistements NSEC3 à un tel dictionnaire.

Validation : Validation, dans le contexte de DNSSEC, se réfère à une des significations suivantes :
* vérifier la validité des signatures DNSSEC,
* vérifier la validité des réponses du DNS, comme celles qui incluent un déni d'existence authentifié, ou
* construire une chaîne d'authentification à partir d'une ancre de confiance jusqu'à une réponse du DNS ou des RRsets DNS individels dans une réponse

Les deux premières définitions ci-dessus considèrent seulement la validité des compoasants DNSSEC individuels comme la validité du RRSIG ou la validité de la preuve NSEC. La troisième définition considère les composants de la chaîne d'authentification DNSSEC entière ; donc, elle exige "une connaissance configurée d'au moins un RR DNSKEY ou DR authentifié" (comme décrit dans la [RFC4035], Section 5).

La [RFC4033], Section 2, dit qu'un "résolveur d'extrémité validant à capacité de sécurite ... effectue la validation de signature" et utilise une ancre de confiance "comme point de départ pour la construction de la chaîne d'authentification d'une réponse DNS signée" ; donc, il utilise la première et la troisième des définitions ci-dessus. Le processus de validation d'un enregistrement de ressource RRSIG est décrit dans la [RFC4035], paragraphe 5.3.

La [RFC5155] se réfère aux réponses de validation tout au long du document, dans le contexte de hachage de déni d'existence authentifié ; cela utilise la seconde définition ci-dessus.

Le terme "authentification" est utilisé de façon interchangeable avec "validation", dans le sens de la troisième définition ci-dessus. La [RFC4033], Section 2, décrit la chaîne qui relie l'ancre de confiance aux données du DNS comme la "chaîne d'authentification". Une réponse est considérée comme authentique si "tous les RRsets dans les sections Réponse et Autorité de la réponse [sont considérés] comme authentiques". (Cité de la [RFC4035]). Les données ou les réponses du DNS réputées être authentiques ou validées ont un état de sécurité de "sûres" ([RFC4035], paragraphe 4.3 ; [RFC4033], Section 5). "Authentifier à la fois les clés et les données du DNS est l'affaire de la politique locae, qui peut étendre ou même supplanter les extensions de protocole de [DNSSEC] ...". (Cité de la [RFC4033], paragraphe 3.1)

Le terme "vérification", quand il est utilisé, est généralement synonyme de "validation".

Résolveur validant *(Validating resolver)* : serveur de noms récurrent à capacité de sécurité, résolveur à capacité de sécurité, ou résolveur d'extrémité à capacité de sécurité qui applique au moins une des définitions de validation (ci-dessus) comme approprié au contexte de résolution. Pour la même raison que le terme générique de "résolveur" est parfois ambigu et doit être évalué dans le contexte (voir la Section 6), "résolveur valideur" est un terme sensible au contexte.

Clé de signature de clé (KSK, *Key signing key*) : clés DNSSEC qui "signent seulement le RRset DNSKEY apex dans une zone". (Cité de la [RFC6781], paragraphe 3.1).

Clé de signature de zone (ZSK, *Zone signing key*) : clés "DNSSEC qui peuvent être utilisées pour signer tous les RRsets dans une zone qui exige des signatures, autres que le RRset DNSKEY apex". (Cité de la [RFC6781], paragraphe 3.1). Noter aussi qu'une ZSK est parfois utilisée pour signer le RRset DNSKEY apex.

Clé de signature combinée *(CSK, combined signing key)* : "dans les cas où la différenciation entre la KSK et la ZSK n'est pas faite, c'est-à-dire, quand les clés ont le rôle à la fois de KSK et de ZSK, on parle d'un schéma de signature d'un seul type *(Single-Type Signing Scheme)*." (Cité de la [RFC6781], paragraphe 3.1). Ceci est parfois appelé une "clé de signature combinée " ou "CSK". C'est une pratique opérationnelle, pas le protocole, qui détermine si une clé particulière est une ZSK, une KSK, ou une CSK.

Point d'entrée sûr (SEP, *Secure Entry Point*) : fanion dans le RDATA DNSKEY qui "peut être utilisé pour distinguer entre les clés qui sont destinées à être utilisées comme point d'entrée sûr dans la zone lors de la construction de la chaîne de confiance, c'est-à-dire, qu'elles doivent être pointées par les RR DS parents ou configurées comme ancre de confiance.... Donc, il est suggéré que le fanion SEP soit établi sur les clés qui sont utilisées comme KSK et pas sur les clés qui sont utilisées comme ZSK, tandis que dans les cas où une distinction entre une KSK et une ZSK n'est pas faite (c'est-à-dire, pour un schéma de signature d'un seul type) il est suggéré que le fanion SEP soit établi sur toutes les clés." (Cité de la [RFC6781], paragraphe 3.2.3). Noter que le fanion SEP est seulement une indication, et que sa présence ou absence ne peut pas être utilisée pour disqualifier un certain RR DNSKEY comme KSK ou ZSK durant la validation.

La définition originale des SEP était dans la [RFC3757]. Cette définition indiquait clairement que le SEP était une clé, pas juste un bit dans la clé. Le résumé de la [RFC3757] dit : "Avec l'enregistrement de ressource (RR, *resource record*) Signataire de délégation (DS, *Delegation Signer*) le concept d'une clé publique agissant comme un point d'entrée sûr a été introduit. Durant les échanges de clés publiques avec le parent, il est nécessaire de différencier les clés SEP des autres clés publiques dans l'ensemble d'enregistrements de ressource DNSKEY (Clé du système des noms de domaines). Un bit fanino dans le RR DNSKEY est défini comme indiquant que DNSKEY est à utilser comme SEP". Cette définition du SEP comme clé a été rendue obsolète par la [RFC4034],et la définition de la [RFC6781] est cohérente avec la [RFC4034].

Ancre de confiance *(Trust anchor)* : "RR DNSKEY ou hachage de RR DS d'un RR DNSKEY configuré. Un résolveur validant à capacité de sécurité utilise cette clé publique ou hachage comme point de départ pour la construction de la chaîne d'authentification jusqu'à une réponse signée du DNS. En général, un résolveur validant devra obtenir les valeurs initiales

de ses ancres de confiance via des moyens sûrs ou de confiance extérieurs au protocole DNS." (Cité de la [RFC4033], Section 2).

Politique DNSSEC (DP, *DNSSEC Policy*) : déclaration qui "établit les exigences et normes de sécurité à mettre en œuvre pour une zone signée DNSSEC." (Cité de la [RFC6841], Section 2).

Déclaration de pratique DNSSEC (DPS, *DNSSEC Practice Statement*) : "document de divulgation des pratiques qui peuvent prendre en charge DNSSEC et être un document supplémentaire à la politique (si un tel document existe) et qui déclare comment la gestion d'une certaine zone met en œuvre les procédures et contrôles à haut niveau." (Cité de la [RFC6841], Section 2).

Module de sécurité de matériel (HSM, *Hardware security module*) : élément spécialisé de matériel qui est utilisé pour créer des clés pour les signatures et pour signer les messages sans même divulguer la clé privée. Dans DNSSEC, les HSM sont souvent utilisés pour contenir les clés privées pour les KSK et ZSK et pour créer les signatures utilisées dans les enregistrements RRSIG à des intervalles périodiques.

Logiciel de signature *(Signing software)* : les serveurs DNS d'autorité qui prennent en charge DNSSEC contiennent souvent un logiciel qui facilite la création et la maintenance des signatures DNSSEC dans les zones. Il y a aussi des logiciels autonomes qui peuvent être utilisés pour signer une zone sans considération de si le serveur d'autorité prend lui-même en charge la signature. Le logiciel de signature peut prendre en charge des HSM particuliers au titre du processus de signature.

11. États DNSSEC

Un résolveur validant peut déterminer qu'une réponse est dans un des quatre états sûr, non sûr, fautif ou indéterminé. Ces états sont définis dans les [RFC4033] et [RFC4035], bien que les définitions des deux documents diffèrent légèrement. Le présent document ne fait aucun effort pour concilier les définitions des deux documents, et ne prend pas position sur la question de savoir si elles doivent être conciliées.

La Section 5 de la [RFC4033] dit : Un résolveur validant peut déterminer les quatre états suivants :

Sûr : le résolveur validant a une ancre de confiance, une chaîne de confiance, et est capable de vérifier toutes les signatures dans les réponses.

Non sûr : le résolveur validant a une ancre de confiance, une chaîne de confiance, et, à un certain point de délégation, une preuve signée de la non existence d'un enregistrement de DS. Cela indique que des branches ultérieures de l'arborescence sont d'une insécurité prouvée. Un résolveur validant peut avoir une politique locale pour marquer des parties de l'espace du domaine comme non sûres.

Fautif : le résolveur validant a une ancre de confiance et une délégation sûre qui indique que les données subsidiaires sont signées, mais que la réponse a échoué à les valider pour une raison quelconque : signatures manquantes, signatures périmées, signatures avec des algorithmes non pris en charge, données manquantes dont le RR NSEC pertinent dit qu'elles devraient être présentes, et ainsi de suite.

Indéterminé : il n'y a pas d'ancre de confiance qui indiquerait qu'une portion spécifique de l'arborescence est sûre. C'est le mode de fonctionnement par défaut.

Le paragraphe 4.3 de la [RFC4035] dit : un résolveur à capacités de sécurité doit être capable de distinguer quatre cas :

Sûr : un RRset pour lequel le résolveur est capable de construire une chaîne de RR DNSKEY et DS signés depuis une ancre de sécurité de confiance jusqu'au RRset. Dans ce cas, le RRset devrait être signé et est soumis à validation de signature, comme décrit ci-dessus.

Non sûr : un RRset pour lequel le résolveur sait qu'il n'y a pas de chaîne de RR DNSKEY et DS signés à partir un point de départ de confiance jusqu'au RRset. Cela peut se produire lorsque le RRset cible se trouve dans une zone non signée ou dans un descendant d'une zone non signée. Dans ce cas, le RRset peut ou non être signé, mais le résolveur ne sera pas capable de vérifier la signature.

Fautif : un RRset pour lequel le résolveur estime qu'il devrait être capable d'établir une chaîne de confiance mais pour lequel il est incapable de le faire, soit à cause de signatures qui ont échoué à la validation pour une raison quelconque ou à cause de données manquantes dont les RR DNSSEC pertinents indiquent qu'elles devraient être présentes. Ce cas peut indiquer une attaque mais peut aussi indiquer une erreur de configuration ou une forme de corruption des données.

Indéterminé : un RRset pour lequel le résolveur n'est pas capable de déterminer si le RRset devrait être signé, car le résolveur n'est pas capable d'obtenir les RR DNSSEC nécessaires. Cela peut arriver quand le résolveur à capacités de sécurité n'est pas capable de contacter les serveurs de noms à capacité de sécurité pour les zones pertinentes.

12. Considérations sur la sécurité

Ces définitions ne changent aucune des considérations sur la sécurité pour le DNS.

13. Considérations relatives à l'IANA

Le présent document n'appelle à aucune action de la part de l'IANA.

14. Références

14.1. Références normatives

[IANA_RootFiles] IANA, "Root Files", <https://www.iana.org/domains/root/files >.

[RFC0822] D. Crocker, "Norme pour le format des messages de texte de l'ARPA-Internet", STD 11, août 1982. (*Obsolète, voir RFC*5322), DOI 10.17487/RFC0882, .

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936, 8020, 8482), DOI 10.17487/RFC1034.

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2673, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604, 7766, 8482), DOI 10.17487/RFC1035.

[RFC1123] R. Braden, éditeur, "Exigences pour les hôtes Internet – Application et prise en charge", STD 3, octobre 1989. *(MàJ par* RFC7766), DOI 10.17487/RFC1123.

[RFC1912] D. Barr, "Erreurs opérationnelles et de configuration courantes sur le DNS", février 1996. *(Information)*, DOI 10.17487/RFC1912.

[RFC1996] P. Vixie, "Mécanisme de notification rapide des changements de zone (DNS NOTIFY)", août 1996. *(P.S.),* DOI 10.17487/RFC1996.

[RFC2136] P. Vixie, S. Thomson, Y. Rekhter et J. Bound, "Mises à jour dynamiques dans le système de noms de domaine (DNS UPDATE)", avril 1997, DOI 10.17487/RFC2136.

[RFC2181] R. Elz et R. Bush, "Clarifications pour la spécification du DNS", juillet 1997. *(P.S., MàJ par* RFC4035, RFC2535, RFC4343, RFC4033, RFC4034, RFC5452), DOI 10.17487/RFC2181.

[RFC2182] R. Elz et autres, "Sélection et fonctionnement des serveurs secondaires du DNS", juillet 1997. (BCP0016), DOI 10.17487/RFC2182,.

[RFC2308] M. Andrews, "Mise en antémémoire négative des interrogations du DNS (DNS NCACHE)", mars 1998. (*MàJ par les RFC* 4033, 4034, 4035, 6604, 8020) *(P.S.)*, DOI 10.17487/RFC2308.

[RFC4033] R. Arends, et autres, "Introduction et exigences pour la sécurité du DNS", mars 2005, DOI 10.17487/RFC4033.

[RFC4034] R. Arends et autres, "Enregistrements de ressources pour les extensions de sécurité au DNS", mars 2005, DOI 10.17487/RFC4034.

[RFC4035] R. Arends et autres, "Modifications du protocole pour les extensions de sécurité du DNS", mars 2005. *(P.S. ; MàJ par* RFC8198, DOI 10.17487/RFC4035.

[RFC4592] E. Lewis, "Le rôle des caractères génériques dans le système des noms de domaines", juillet 2006. *(P.S.)*, DOI 10.17487/RFC4592.

[RFC5155] B. Laurie et autres, "Déni d'existence authentifié à hachage de la sécurité du DNS (DNSSEC)", mars 2008. *(P.S.)*, DOI 10.17487/RFC5155.

[RFC5358] J. Damas, F. Nves, "Empêcher l'utilisation de noms de serveurs récurrents dans les attaques par réflecteur", octobre 2008. (BCP0140), DOI 10.17487/RFC5358.

[RFC5730] S. Hollenbeck, "Protocole d'approvisionnement extensible (EPP)", STD0069, août 2009. *(Remplace la* RFC4930), DOI 10.17487/RFC5730.

[RFC5731] S. Hollenbeck, "Protocole d'approvisionnement extensible (EPP) ; Transposition des noms de domaine", STD0069, août 2009. *(Remplace la* RFC4931), DOI 10.17487/RFC5731.

[RFC5855] J. Abley, T. Manderson, "Serveurs de noms pour les zones inverses IPv4 et IPv6", mai 2010. (BCP0155), DOI 10.17487/RFC5855.

[RFC5936] E. Lewis, A. Hoenes, "Protocole de transfert de zone du DNS (AXFR)", juin 2010. (*MàJ* RFC1034, RFC1035). *(P. S.)*, DOI 10.17487/RFC5936.

[RFC6561] J. Livingood, N. Mody, M. O'Reirdan, "Recommandations pour remédier aux zombies dans les réseaux de FAI", mars 2012. *(Information)*, DOI 10.17487/RFC6561.

[RFC6781] O. Kolkman, W. Mekking et R. Gieben, "Pratiques du fonctionnement de DNSSEC, version 2", décembre 2012, DOI 10.17487/RFC6781.

[RFC6840] S. Weiler et D. Blacka, éd., "Précision et notes de mise en œuvre pour la sécurité du DNS (DNSSEC)", février 2013, DOI 10.17487/RFC6840.

[RFC6841] F. Ljunggren, AM. Eklund Lowinder et T. Okubo, "Cadre pour les politiques DNSSEC et les déclarations de pratique de DNSSEC", janvier 2013, DOI 10.17487/RFC6841.

[RFC6891] J. Damas, M. Graff, P. Vixie, "Mécanismes d'extension pour le DNS (EDNS(0))", STD0075, avril 2013. (*Remplace* RFC2671, RFC2673), DOI 10.17487/RFC6891.

[RFC7344] W. Kumari, O. Gudmundsson, G. Barwood, "Automatisation de la maintenance de la délégation de confiance DNSSEC", septembre 2014. *(Information ; MàJ par* RFC8078), DOI 10.17487/RFC7344.

[RFC7719] P. Hoffman, A. Sullivan. K. Fujiwara, "Terminologie du DNS", décembre 2015. *(Information , remplacée par* RFC8499 ; BCP 219*)*, DOI 10.17487/RFC7719.

[RFC8310] S. Dickinson, D. Gillmor, T. Reddy, "Profils d'utilisation pour le DNS sur TLS et DTLS", mars 2018. *(P.S. ; MàJ* RFC7858*)*, DOI 10.17487/RFC8310.

14.2 Références pour information

[IANA-RR] IANA, "Resource Record (RR) TYPEs", <https://www.iana.org/assignments/dns-parameters/ >.

[RFC0819] Z. Su et J. Postel, "Convention de nommage des domaines pour les applications d'utilisateurs de l'Internet", août 1982, DOI 10.17487/RFC0819.

[RFC0952] K. Harrenstien, M. Stahl, E. Feinler, "Spécification du tableau des hôtes de l'Internet du DOD", octobre 1985, DOI 10.17487/RFC0952.

[RFC1713] A. Romao, "Outils pour le débogage du DNS", FYI0027, novembre 1994. *(Information)*, DOI 10.17487/RFC1713.

[RFC1995] M. Ohta, "Transferts de zone par incréments dans le DNS", RFC 1995, août 1996, DOI 10.17487/RFC1995.

[RFC2775] B. Carpenter, "Transparence de l'Internet", février 2000. *(Information)*, DOI 10.17487/RFC2775.

[RFC3172] G. Huston, éd., "Lignes directrice de gestion et exigences opérationnelles pour le domaine ("arpa") de zone d'adresse et de paramètre d'acheminement", septembre 2001. (BCP0052), DOI 10.17487/RFC3172.

[RFC3425] D. Lawrence, "IQUERY est devenu obsolète", novembre 2002. *(P.S.)*, DOI 10.17487/RFC3425.

[RFC3493] R. Gilligan et autres, "Extensions d'interface de prise de base pour IPv6", février 2003. *(Information)*, DOI 10.17487/RFC3493.

[RFC3757] O. Kolkman, J. Schlyter, E. Lewis, "Fanion de pont d'entrée sécurisée (SED) d'enregistrement de ressource (RR) KEY du système de noms de domaines (DNSKEY)", avril 2004. (*Obsolète, voir* RFC4033, RFC4034, RFC4035) *(P.S.)*, DOI 10.17487/RFC3757.

[RFC3912] L. Daigle, "Spécification du protocole WHOIS", septembre 2004. *(D.S.)*, DOI 10.17487/RFC3912.

[RFC4641] O. Kolkman, R. Gieben, "Fonctionnement pratique de DNSSEC", septembre 2006. *(Remplace* RFC2541) *(Information)*, DOI 10.17487/RFC4641.

[RFC4697] M. Larson, P. Barber, "Dysfonctionnements observés de résolution du DNS", octobre 2006. (BCP0123), DOI 10.17487/RFC4697.

[RFC4786] J. Abley, K. Lindqvist, "Fonctionnement des services d'envoi à la cantonade", décembre 2006. (BCP0126), DOI 10.17487/RFC4786.

[RFC4956] R. Arends et autres, "Modèle Opt-in pour la sécurité du DNS (DNSSEC)", juillet 2007. *(Expérimentale)*, DOI 10.17487/RFC4956.

[RFC5625] R. Bellis, "Lignes directrices pour la mise en œuvre de mandataire du DNS", BCP0152, août 2009, DOI 10.17487/RFC5625.

[RFC5890] J. Klensin, "Noms de domaine internationalisés pour les applications (IDNA) : Définitions et cadre documentaire", août 2010. *(Remplace RFC*3490) *(P.S.)*, DOI 10.17487/RFC5890.

[RFC5891] J. Klensin, "Noms de domaine internationalisés pour les applications (IDNA) : Le protocole", août 2010. (*Remplace* FC3490, RFC3491 ; *MàJ* RFC3492 ; *P.S.)*, DOI 10.17487/RFC5891.

[RFC5892] P. Faltstrom, "Codets Unicode et noms de domaine internationalisés pour les applications (IDNA)", août 2010. *(P.S.)*, DOI 10.17487/RFC5892.

[RFC5893] H. Alvestrand, C. Karp, "Écritures de droite à gauche pour les noms de domaine internationalisés pour les applications (IDNA)", août 2010. *(P.S.)*, DOI 10.17487/RFC5893.

[RFC5894] J. Klensin, "Noms de domaine internationalisés pour les applications (IDNA) : Fondements, explication, et motivations", août 2010. *(Information)*, DOI 10.17487/RFC5894.

[RFC6055] D. Thaler, J. Klensin, S. Cheshire. "Réflexions de l'IAB sur les codages des noms de domaines internationalisés", février 2011. (*MàJ* RFC2130) *(Information)*, DOI 10.17487/RFC6055.

[RFC6265] A. Barth, "Mécanisme de gestion d'état HTTP", avril 2011. *(Remplace* RFC2965 ; *P.S.)*, DOI 10.17487/RFC6265.

[RFC6303] M. Andrews, "Zones du DNS servies localement", juillet 2011. (BCP0163), DOI 10.17487/RFC6303.

[RFC6335] M. Cotton et autres, "Procédures de l'autorité d'allocation des numéros de l'Internet (IANA) pour la gestion du registre des numéros d'accès aux noms de service et protocoles de transport", août 2011. *(MàJ* RFC2780, RFC2782, RFC3828, RFC4340, RFC4960, RFC5595) (BCP0165), DOI 10.17487/RFC6335.

[RFC6365] P. Hoffman, J. Klensin, "Terminologie utilisée dans l'internationalisation à l'IETF", septembre 2011. (*Remplace la* RFC3536) (BCP0166), DOI 10.17487/RFC6365.

[RFC6672] S. Rose, W. Wijngaards, "Redirection DNAME dans le DNS", juin 2012. (*Remplace* RFC2672) (*MàJ*

RFC3363 ; *P.S.)*, DOI 10.17487/RFC6672.

[RFC6762] S. Cheshire et M. Krochmal, "DNS en diffusion groupée", février 2013, DOI 10.17487/RFC6762.

[RFC7129] R. Gieben, W. Mekking, "Déni d'existence authentifié dans le DNS", février 2014. *(Information)*, DOI 10.17487/RFC7129.

[RFC7480] A. Newton, B. Ellacott, N. Kong, "Utilisation de HTTP dans le protocole d'accès aux données d'enregistrement (RDAP)", mars 2015. *(P.S.)*, DOI 10.17487/RFC7480.

[RFC7481] S. Hollenbeck, N. Kong, "Services de sécurité pour RDAP" mars 2015. *(P.S.)*, DOI 10.17487/RFC7481.

[RFC7482] A. Newton, S. Hollenbeck, "Format d'interrogation pour RDAP", mars 2015. *(P.S.)*, DOI 10.17487/RFC7482.

[RFC7483] A. Newton, S. Hollenbeck, "Réponses JSON pour RDAP", mars 2015. *(P.S.)*, DOI 10.17487/RFC7483.

[RFC7484] M. Blanchet, "Trouver le serveur RDAP d'autorité", mars 2015. *(P.S.)*, DOI 10.17487/RFC7484.

[RFC7485] L. Zhou, et autres, "Inventaire et analyse des objets d'enregistrement de WHOIS", mars 2015. *(Information)*, DOI 10.17487/RFC7485.

[RFC7793] M. Andrews, "Ajout de préfixes 100.64.0.0/10 au registre des zones DNS servies localement par IPv4", mai 2016. BCP163, DOI 10.17487/RFC7793.

[RFC7858] Z. Hu, et autres, "Spécification pour le DNS sur TLS", mai 2016. *(P.S. ; MàJ par* RFC8310, 8331), DOI 10.17487/RFC7858.

[RFC8094] T. Reddy, D. Wing, P. Patil, "Sécurité de couche transport de datagramme (DTLS) pour le DNS", février 2017. *(Exp)*, DOI 10.17487/RFC8094.

[RFC8109] P. Koch, M. Larson, P. Hoffman, "Initialisation d'un résolveur DNS avec des interrogations d'amorçage", mars 2017. BCP209, DOI 10.17487/RFC8109.

[RFC8484] P. Hoffman, P. McManus, "Interrogations au DNS sur HTTPS", octobre 2018. *(P.S.)*, DOI 10.17487/RFC8484.

[RSSAC026] Root Server System Advisory Committee (RSSAC), "RSSAC Lexicon", 2017, <https://www.icann.org/en/system/files/files/rssac-026-14mar17-en.pdf >.

Appendice A. Définitions mises à jour par ce document

Les définitions suivantes provenant de RFC sont mises à jour par ce document :

- Transmetteur *(Forwarder)* dans la [RFC2308]
- QNAME dans la [RFC2308]
- Point d'entrée sûr (SEP, *Secure Entry Point*) dans la [RFC3757] ; noter cependant que cette RFC est déjà rendue obsolète (voir les [RFC4033], [RFC4034], [RFC4035]).

Appendice B. Définitions originales du présent document

Les définitions suivantes sont définies pour la première fois dans ce document :

- "Alias" à la Section 2
- "Apex" à la Section 7
- "arpa" à la Section 7
- "Bailiwick" à la Section 7
- "Class independent" à la Section 5
- "Delegation-centric zone" à la Section 7

Index

Remerciements

Ce qui suit est la section remerciements de la RFC 7719.

Les auteurs témoignent de leur reconnaissance à l'égard des auteurs des RFC en rapport avec le DNS qui ont précédées celle-ci. Des commentaires de Tony Finch, Stephane Bortzmeyer, Niall O'Reilly, Colm MacCarthaigh, Ray Bellis, John Kristoff, Robert Edmonds, Paul Wouters, Shumon Huque, Paul Ebersman, David Lawrence, Matthijs Mekking, Casey Deccio, Bob Harold, Ed Lewis, John Klensin, David Black, et de nombreux autres du groupe de travail DNSOP ont aidé à mettre en forme la RFC 7719.

La plupart des changements majeurs entre la RFC 7719 et le présent document viennent d'actives discussion au sein du groupe de travail DNSOP. Les personnes spécifiques qui ont contribué matériellement au présent document sont : Bob Harold, Dick Franks, Evan Hunt, John Dickinson, Mark Andrews, Martin Hoffmann, Paul Vixie, Peter Koch, Duane Wessels, Allison Mankin, Giovane Moura, Roni Even, Dan Romascanu, et Vladmir Cunat.

Adresse des auteurs

Kazunori Fujiwara
Japan Registry Services Co., Ltd.
Chiyoda First Bldg. East 13F, 3-8-1 Nishi-Kanda
Chiyoda-ku, Tokyo 101-0065
Japan
mél : fujiwara@jprs.co.jp

Paul HoffmanI
ICANN
mél : paul.hoffman@icann.org

Andrew Sullivan
mél : ajs@anvilwalrusden.com