Internet
made in France

La lettre n°8

01

DELEG, le projet qui promet de faire évoluer la délégation DNS

Le projet DELEG, récemment structuré en groupe de travail au sein de l'IETF *(Internet Engineering Task Force)*, promet de transformer en profondeur la façon dont la délégation DNS fonctionne aujourd'hui. Ce mécanisme, qui permet la décentralisation de la gestion des noms de domaine et sous-domaines sur internet, repose sur des pratiques établies depuis des décennies. Mais dans le monde moderne, celles-ci affichent désormais certaines limites.

Alors que les travaux ne font que commencer au sein de l'IETF, c'est précisément le moment pour la communauté technique et les parties prenantes de s'impliquer, influencer ainsi les spécifications de la future norme technique et garantir que cette refonte réponde aux besoins de l'écosystème DNS *(Domain Name System)* dans son ensemble.

Qu'est-ce que la délégation DNS ?

Prérequis : la structure hiérarchique du DNS

Avant d'aborder le mécanisme de délégation DNS, il est nécessaire de comprendre comment un nom de domaine est structuré. Un nom de domaine est en effet composé de plusieurs niveaux, appelés « composants » et séparés par des points. Le composant situé à la fin d'un nom de domaine, souvent appelé « extension », doit être choisi parmi une liste officielle de domaines de premier niveau (*Top-Level Domains* ou TLD), tels que .fr, .org ou .com. Les composants suivants forment le reste du nom de domaine : dans la majorité des cas, ils définissent le domaine de deuxième niveau (*Second-Level Domain* ou SLD) et, le cas échéant, les sous-domaines.

La structure des noms de domaine va au-delà de la simple convention syntaxique : elle reflète également l'organisation hiérarchique de l'infrastructure du DNS qui permet de gérer et résoudre les noms de domaine. Chaque niveau d'un nom de domaine correspond à un niveau dans cette hiérarchie technique qui peut être comparée à celle d'un arbre inversé, de la racine située au sommet, jusqu'au dernier des sous-domaines :

- **La racine.** Située au sommet de la hiérarchie DNS, la racine est composée de 13 serveurs répartis dans le monde, qui orientent les requêtes des internautes vers les serveurs DNS des domaines de premier niveau. Bien qu'ils ne détiennent pas directement les informations sur les domaines spécifiques, ils constituent le point de départ pour toutes les requêtes DNS.
- **Les domaines de premier niveau.** Juste en dessous de la racine se trouvent les TLD, chacun d'entre eux étant géré par un registre, tel l'Afnic pour le .fr. Ces registres exploitent des serveurs DNS qui fournissent les informations nécessaires pour identifier les domaines de deuxième niveau enregistrés sous le TLD.
- **Les domaines de deuxième niveau.** Situés directement sous un TLD, les domaines de deuxième niveau, comme « exemple.fr », sont enregistrés par des entreprises, organisations ou particuliers. Il s'agit de la composante personnalisable d'une adresse web que l'on appelle également nom de domaine.
- **Les sous-domaines.** Plus bas dans la hiérarchie se trouvent les sous-domaines, qui sont des subdivisions des domaines de deuxième niveau ou d'autres sous-domaines. Par exemple, « blog.exemple.fr » est un sous-domaine de « exemple.fr », d'ailleurs lui-même un sous-domaine de « .fr ». Les sous-domaines permettent notamment de structurer des services (comme un blog ou un service de messagerie).

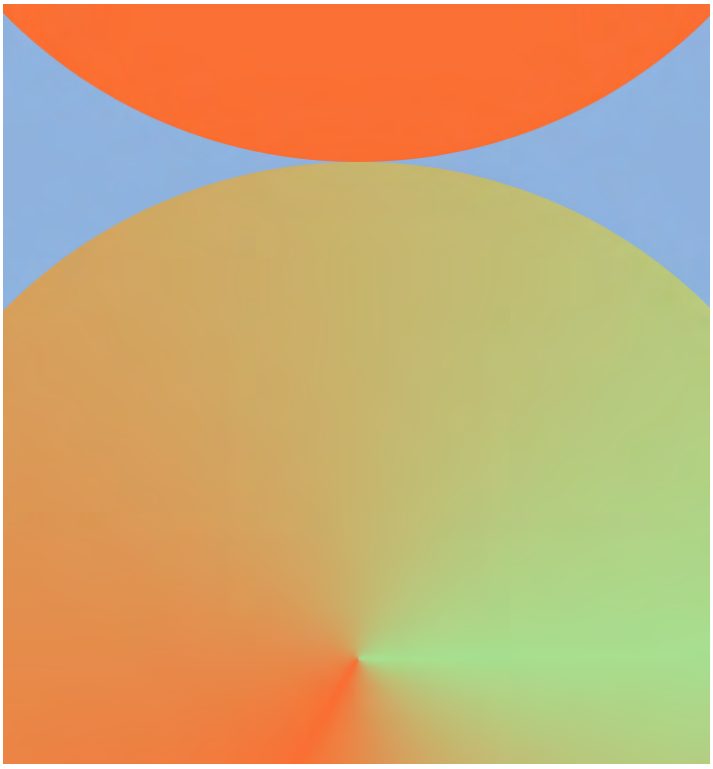
Qu'est-ce qui peut être délégué ?

Dans la hiérarchie DNS, chacun des niveaux offre la possibilité de déléguer la gestion de la zone située en dessous. C'est ce qu'on appelle la délégation DNS, mécanisme qui consiste à confier la responsabilité technique et/ou administrative d'une « zone fille » à une entité différente de celle qui gère la « zone parent ».

Ce transfert de responsabilité est au cœur de l'architecture décentralisée du DNS. Lorsqu'une zone est déléguée, l'entité qui la reçoit obtient l'autorité sur cette partie de l'espace des noms de domaine, y compris sur la création et la gestion de sous-domaines, à moins que ces derniers ne soient à leur tour délégués.

Ainsi, la racine délègue les TLD aux registres, les registres délèguent les domaines de deuxième niveau à leurs titulaires, et ces derniers peuvent déléguer des sous-domaines si nécessaire. À chaque étape, la délégation transfère non seulement la responsabilité de la zone déléguée, mais aussi l'autonomie de gérer ce qui se trouve en dessous.

Cette capacité à déléguer à chaque niveau garantit la flexibilité et l'évolutivité du système DNS, tout en respectant sa structure hiérarchique.



À quoi sert la délégation DNS ?

La délégation DNS joue un rôle très important dans le fonctionnement d'internet, en assurant la décentralisation, l'évolutivité et la flexibilité de la gestion des noms de domaine. Elle permet en effet à chaque entité de gérer son propre domaine ou sous-domaine avec une grande autonomie. Une fois qu'un domaine est délégué, son titulaire peut prendre des décisions de manière indépendante : il peut ajouter de nouveaux sous-domaines, modifier les configurations DNS ou gérer les services associés, et ce, sans devoir obtenir l'approbation du domaine parent.

Cela permet notamment aux organisations de structurer plus facilement leurs activités en ligne. Ainsi, une université peut utiliser « bibliotheque.universite.fr » pour son catalogue numérique et « mail.universite.fr » pour ses serveurs de messagerie, rendant la gestion des services plus intuitive et plus facile à configurer.

En répartissant la gestion des sous-domaines sur différents serveurs DNS, la délégation améliore également la résilience et la performance du système. Cette répartition diminue les risques de surcharge ou de panne globale, et garantit que chaque entité peut gérer sa zone DNS de manière indépendante, renforçant ainsi la robustesse du système dans son ensemble.

Enfin, la délégation DNS permet à internet de s'adapter à sa propre croissance. Avec des centaines de millions de noms de domaine actifs aujourd'hui, confier la gestion des sous-domaines à différents acteurs permet de faire évoluer les ressources au rythme des besoins, là où une gestion centralisée serait impraticable à cette échelle.

Quelles sont les limites de la délégation DNS aujourd'hui ?

En place depuis des décennies, le système de délégation DNS reflète aujourd'hui encore les choix de conception d'une époque où le réseau était moins vaste et moins complexe. Avec l'évolution rapide d'internet, le mécanisme montre aujourd'hui certaines limites.

Problèmes de synchronisation entre zone parent et zone fille

Lorsque la gestion d'une zone est déléguée, des informations importantes sont maintenues simultanément dans deux endroits : la zone parent, qui contient des informations indiquant quels serveurs sont responsables de la zone déléguée ; la zone fille, qui gère ces serveurs et leurs enregistrements DNS de manière autonome.

Pour que le système fonctionne correctement, ces informations doivent rester parfaitement synchronisées entre les deux zones. Cependant, dans la pratique, il arrive que les données soient mal alignées, la gestion manuelle de cette synchronisation pouvant entraîner des erreurs, des délais ou des incohérences. Ainsi, si la zone parent référence des serveurs qui ne sont plus d'actualité dans la zone fille, les requêtes DNS peuvent échouer ou être redirigées incorrectement.

Des informations limitées dans les enregistrements NS

Les enregistrements NS (*Name Server*), qui spécifient les serveurs DNS faisant autorité pour une zone donnée, sont essentiels pour la délégation DNS. Ils ne fournissent cependant que les noms des serveurs, sans offrir la possibilité d'y ajouter des informations supplémentaires qui pourraient être utiles dans le contexte actuel. Par exemple :

- **Les protocoles sécurisés.** Les serveurs DNS modernes peuvent prendre en charge des protocoles sécurisés comme DNS-over-TLS (DoT) ou DNS-over-HTTPS (DoH), qui chiffrent les communications pour plus de sécurité. Or, les enregistrements NS ne permettent pas d'indiquer si ces fonctionnalités sont disponibles sur le serveur ciblé. Cela complique leur adoption et limite la capacité des utilisateurs à tirer parti de ces protections.
- **Les configurations personnalisées.** Par exemple, si un serveur DNS utilise un port réseau différent du port standard (port 53), cette information ne peut pas être incluse dans les enregistrements NS. Cela peut rendre difficile la configuration ou l'utilisation de certains serveurs.

La gestion délicate des enregistrements Glue

Les enregistrements Glue (ou « colle ») répondent au problème – souvent appelé « *problème de l'œuf et de la poule* » – de dépendance circulaire dans le système DNS lorsqu'un serveur DNS faisant autorité pour une zone se trouve dans cette même zone. Les résolveurs DNS peuvent alors peiner à récupérer les informations nécessaires pour résoudre un nom de domaine : pour interroger un serveur DNS, ils doivent en effet connaître son adresse IP ; mais comme cette information se situe dans la zone administrée par ce même serveur, ils ne peuvent y accéder sans l'interroger au préalable, ce qui crée un cercle vicieux.

Pour résoudre ce problème, la zone parent conserve une copie des adresses IP des serveurs DNS concernés : c'est ce qu'on appelle la « colle ». Il est à noter que les enregistrements de colle dans la zone parent ne font pas autorité ; ils ne sont que des copies des informations faisant autorité contenues dans la zone fille.

Si cette colle permet de briser le cercle vicieux, elle présente des inconvénients. En cas de changement d'adresse IP d'un serveur DNS dans la zone fille, la colle dans la zone parent doit être mise à jour manuellement. Cette étape est parfois oubliée, entraînant des risques de désynchronisation.

DNSSEC et mise à jour des enregistrements DS

Les enregistrements DS *(Delegation Signer)* sont utilisés dans le cadre de DNSSEC, une extension du DNS qui garantit l'authenticité et l'intégrité des échanges DNS grâce à des signatures cryptographiques, pour sécuriser les relations entre zone parent et zone fille. Ces enregistrements DS ne se trouvent que dans la zone parent. Cela signifie que toute modification des clés DNSSEC dans la zone fille nécessite une mise à jour des enregistrements DS dans la zone parent, souvent via un processus manuel impliquant plusieurs parties, pouvant donc engendrer les mêmes problèmes d'erreur et de synchronisation.

Tous les hébergeurs DNS ne peuvent pas directement modifier les enregistrements DNS

Dans le système DNS, les serveurs faisant autorité pour une zone peuvent être gérés par différents types d'hébergeurs DNS. Ils peuvent être le bureau d'enregistrement (BE), une organisation tierce spécialisée dans l'hébergement DNS, ou même le titulaire du domaine lui-même. Cependant, lorsqu'un hébergeur DNS est distinct du registre, du BE ou du titulaire, son rôle se limite à la gestion technique des serveurs de noms. Il ne peut pas modifier directement les enregistrements DNS critiques, tels que les enregistrements NS ou DS, car ces modifications nécessitent l'intervention du titulaire et/ou du BE auprès du registre.

Ce fonctionnement, bien qu'il garantisse la sécurité et l'intégrité du système DNS, est source d'une certaine complexité. Si un hébergeur DNS souhaite, par exemple, ajouter ou modifier un serveur de noms dans sa configuration, il doit en informer le titulaire du domaine, qui transmettra la demande au BE, puis au registre. Cette chaîne de communication peut ralentir les modifications nécessaires, augmenter les risques d'erreurs et compliquer la gestion des zones DNS.

DELEG : une solution pour moderniser la délégation DNS

Face aux limites techniques et organisationnelles identifiées dans le système actuel, le projet DELEG propose de moderniser en profondeur la délégation DNS en créant un nouveau type d'enregistrements, appelés enregistrements DELEG.

Des enregistrements enrichis

Les enregistrements DELEG sont conçus pour remplacer ou compléter les enregistrements NS actuels dans la zone parent. Contrairement aux enregistrements NS, qui se limitent à fournir les noms des serveurs DNS responsables de la zone fille, les enregistrements DELEG prévoient d'inclure des informations supplémentaires sur la zone déléguée, telles que :

- Les adresses IP des serveurs DNS, évitant ainsi de devoir les résoudre séparément.
- Les protocoles sécurisés pris en charge, comme DNS-over-TLS (DoT) ou DNS-over-HTTPS (DoH).
- Les ports spécifiques utilisés par les serveurs DNS.
- Toute autre information nécessaire pour améliorer la résolution DNS ou faciliter l'adoption de nouvelles technologies, aujourd'hui et à l'avenir.

Une meilleure synchronisation entre zones parent et fille

L'un des principaux problèmes du système actuel est le besoin de synchroniser manuellement les informations entre la zone parent et la zone fille. Le projet DELEG propose de résoudre ce problème grâce à un mécanisme de « pointeur ».

> **Le projet DELEG propose de résoudre ce problème grâce à un mécanisme de « pointeur ».**

Les enregistrements DELEG, situés dans la zone parent, renverront directement vers les informations stockées dans la zone fille, évitant ainsi les dépendances liées à la duplication des données.

Une gestion simplifiée pour les hébergeurs DNS

Avec DELEG, les hébergeurs DNS, même tiers, pourraient jouer un rôle plus direct et autonome dans la gestion des délégations. Les enregistrements DELEG leur offriraient la possibilité de transmettre les informations nécessaires directement à la zone parent, simplifiant ainsi les mises à jour et éliminant les délais causés par les intermédiaires.

Une transformation ambitieuse et nécessaire, qui se décide aujourd'hui

Le projet DELEG n'est pas simplement une évolution technique du DNS ; il marque une tentative de modernisation profonde, visant à résoudre des problèmes structurels tout en ouvrant de nouvelles perspectives pour l'écosystème internet. En proposant la création d'un nouveau type d'enregistrements, DELEG promet de rendre la délégation DNS plus fiable, plus flexible et plus adaptée aux défis du futur.

Cependant, cette transformation ne se fera pas sans effort. Mettre en œuvre DELEG implique de repenser et de mettre à jour une chaîne entière d'outils et de systèmes : des serveurs DNS aux résolveurs, en passant par les interfaces des bureaux d'enregistrement et les protocoles associés. Ce travail nécessite une coordination étroite entre les différents acteurs de l'écosystème – des registres aux opérateurs DNS, en passant par les développeurs d'outils techniques.

La période de transition, durant laquelle les mécanismes actuels (comme les enregistrements NS) coexisteront avec DELEG, soulèvera encore d'autres défis : synchronisation des données, gestion de deux systèmes en parallèle, adoption progressive par des infrastructures variées… Ces étapes devront être soigneusement planifiées pour éviter tout impact négatif sur la stabilité du DNS.

Malgré ces obstacles, DELEG représente aujourd'hui une véritable opportunité pour les acteurs du DNS de façonner un système encore plus robuste, durable et évolutif.
Avec le lancement des travaux au sein de l'IETF, les contours de la future norme technique commencent à se dessiner.
Si ce projet aboutit, il pourrait transformer en profondeur la délégation DNS, entraînant des ajustements importants dans les pratiques et les outils de l'écosystème. Mieux comprendre ces évolutions dès maintenant permettra à chacun d'anticiper les impacts qu'elles pourraient avoir à l'avenir.

2

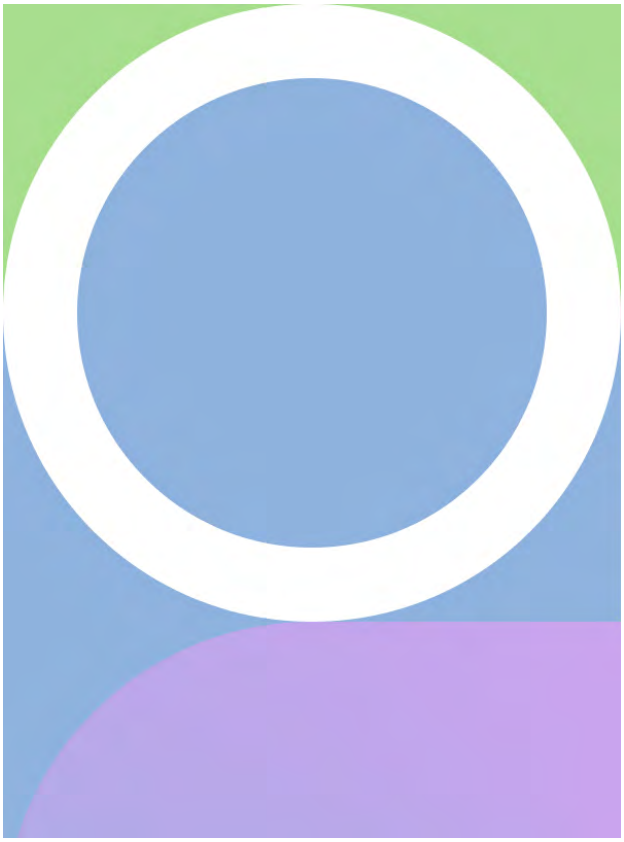
Assemblée mondiale de normalisation des télécommunications : l'édition 2024 réaffirme les principes d'un internet inclusif, résilient et durable

La 25e édition de l'Assemblée mondiale de normalisation des télécommunications (AMNT, en anglais *World Telecommunication Standardization Assembly* ou WTSA) s'est tenue pour la première fois sur le continent asiatique, à New Delhi en Inde, en octobre 2024. Organisé tous les quatre ans par l'Union Internationale des Télécommunications (UIT), cet événement rassemble les membres de l'Union, des experts et décideurs du monde entier pour définir les grandes orientations de la normalisation des télécommunications.

Le rendez-vous incontournable du secteur de la normalisation des télécommunications (UIT-T)

L'Union Internationale des Télécommunications est l'agence spécialisée des Nations Unies en charge des Technologies de l'information et de la communication. Elle est structurée en trois secteurs : Radiocommunication (UIT-R), pour la gestion des fréquences radio et des orbites satellitaires ; Développement des télécommunications (UIT-D), qui promeut un accès équitable et durable aux technologies ; Normalisation des télécommunications (UIT-T), qui élabore des normes techniques internationales. Ces trois secteurs travaillent en synergie pour garantir que les avancées technologiques dans le domaine des télécommunications profitent au plus grand nombre, tout en répondant à des enjeux de durabilité, d'éthique et de sécurité.

C'est du secteur « T », qui se consacre à l'élaboration des normes internationales pour garantir l'interopérabilité des systèmes de télécommunication, que relève l'AMNT. Cette assemblée joue un rôle stratégique en définissant, tous les quatre ans, les priorités et les orientations pour les travaux de normalisation conduits par l'UIT dans la prochaine période d'étude. Elle rassemble des experts techniques, des décideurs politiques et des représentants du secteur afin de coordonner les efforts de tous face aux défis des télécommunications que sont l'évolution rapide des technologies, l'émergence de nouveaux usages numériques, la durabilité dans le secteur des télécommunications et la nécessité de garantir une connectivité inclusive. En réunissant régulièrement toutes les parties prenantes, l'AMNT favorise une collaboration internationale harmonisée afin de relever conjointement ces défis.



AMNT-24, une édition marquée par une forte participation

L'AMNT-24 a réuni près de 3 700 participants de 164 pays, un chiffre record. La conférence a été inaugurée par le Premier ministre indien, Narendra Modi, soulignant l'importance de l'événement pour le pays hôte, dans un contexte de montée en puissance de l'Asie – et plus spécifiquement de l'Inde – dans le domaine numérique.

La délégation française, dirigée par l'ambassadeur Éric Fournier, s'est distinguée dans les discussions liées à l'environnement, au climat et à l'économie circulaire, ainsi que regardant les résolutions internet et la défense du modèle multipartite de la gouvernance d'internet. L'Afnic a contribué activement à ces échanges, notamment en défendant une vision d'un internet respectueux de l'environnement et de la diversité linguistique et culturelle.

> **Une vision d'un internet respectueux de l'environnement et de la diversité linguistique et culturelle.**

Tout au long de l'événement, ces contributions se sont inscrites dans un dialogue plus large, touchant toutes les facettes de la normalisation des télécommunications, avec des thématiques englobant tout aussi bien la qualité de service que la sécurité des réseaux ou encore la tarification. Ces discussions ont conduit à l'adoption ou à la révision des résolutions de l'UIT-T, mettant en lumière les priorités stratégiques et les réponses collectives aux enjeux technologiques, économiques et sociétaux des télécommunications.

Résolutions majeures et priorités stratégiques

Le compte-rendu officiel de l'AMNT-24 donne une vue d'ensemble des nombreuses résolutions adoptées ou révisées lors de l'assemblée. Ces textes abordent des sujets variés : normalisation technique, transition vers IPv6, technologies émergentes comme l'internet des objets ou l'intelligence artificielle, durabilité environnementale…

Parmi toutes ces résolutions, certaines ont un lien direct avec internet et ses infrastructures, notamment le DNS. Ce sont ces sujets que l'Afnic a particulièrement suivis et pour lesquels elle s'est investie lors des discussions. Voici les résolutions les plus marquantes.

- **Résolution 47 – Noms de domaine de premier niveau de type code de pays**

  Cette résolution, qui n'a pas été modifiée depuis 2012, reste un socle pour les domaines de premier niveau nationaux (ccTLD) tels que le .fr. Elle souligne leur rôle essentiel en tant qu'infrastructures nationales dans les écosystèmes numériques, garantissant la souveraineté numérique des États et un accès local sécurisé à internet. Conserver cette résolution inchangée permet de réitérer le consensus sur les organisations compétentes en matière de noms de domaine et sur la souveraineté des États sur leur ccTLD.

- **Résolution 48 – Noms de domaine internationalisés (et multilingues)**

  Cette résolution a été actualisée pour réaffirmer l'importance du multilinguisme dans l'écosystème internet et encourager une collaboration renforcée entre les acteurs concernés afin de faciliter l'adoption des noms de domaine internationalisés (IDN). Est ainsi mentionné le rôle que jouent le secteur privé, les organisations régionales et internationales concernées et la communauté des opérateurs de domaine de premier niveau en la matière, notamment à travers des initiatives telles que la Coalition pour une Afrique numérique. L'évolution de cette résolution fait écho plus largement aux discussions en matière de diversité linguistique sur internet, essentielle pour favoriser la diversité culturelle.

  Ce sujet, qui vise à rendre internet accessible à toutes les communautés linguistiques, notamment celles utilisant des scripts non latins, fait l'objet d'un article « *Universal Acceptance : les défis d'un internet linguistiquement inclusif* », publié dans La Lettre Afnic #4.

- **Résolution 64 – Promouvoir, faciliter et accélérer le passage à la version 6 du protocole Internet ainsi que le déploiement de ce protocole**

  Cette résolution, mise à jour pour refléter les avancées technologiques, vise à accélérer le déploiement mondial d'IPv6, le protocole de communication conçu pour remplacer IPv4. Ce dernier, en place depuis les débuts d'internet, est limité à environ 4,3 milliards d'adresses IP en raison de sa structure basée sur des adresses codées sur 32 bits. Ce nombre est aujourd'hui insuffisant face à l'explosion des appareils connectés. IPv6, avec sa capacité à générer un nombre quasiment illimité d'adresses uniques grâce à un codage sur 128 bits, permet en revanche d'assurer la stabilité et l'expansion d'internet.

  La résolution actualisée insiste également sur la collaboration internationale, le partage de bonnes pratiques notamment en ce qui concerne la passation de marchés publics, la sensibilisation et la formation pour surmonter les défis techniques et infrastructurels, afin de faciliter et optimiser la transition d'IPv4 à IPv6.

- **Résolution 73 – Les technologies de l'information et de la communication, l'environnement, les changements climatiques et l'économie circulaire**

  Cette résolution insiste sur la nécessité de mesurer et réduire l'impact environnemental des technologies numériques. Elle reconnaît que, bien qu'essentielles à la transformation numérique, elles doivent être intégrées dans une logique de durabilité.

  Sur ce sujet, la Commission d'étude 5 (CE 5) a été confirmée comme structure clé pour piloter les travaux. À sa tête, le Français Dominique Wurges, Directeur des relations institutionnelles et de la normalisation au sein du Département Innovation d'Orange, a été réélu comme Président lors de l'AMNT. Cette commission de l'UIT est dédiée aux questions environnementales liées aux nouvelles technologies, avec pour mission de développer des normes techniques visant à réduire l'empreinte carbone des infrastructures numériques, à promouvoir une meilleure efficacité énergétique et à encourager des pratiques relevant de l'économie circulaire.

  La résolution actualisée met également l'accent sur la collaboration internationale et le partage de bonnes pratiques, intègre la dimension multicritère de ces impacts environnementaux et la prise en compte de la totalité du cycle de vie des infrastructures techniques.

  L'Afnic est fortement engagée sur ces enjeux : elle participe activement aux discussions au sein de la CE 5 et a également développé des outils spécifiques pour mesurer l'impact environnemental du DNS (lire à ce sujet l'article *« Impact environnemental du DNS : où en est-on ? »* publié dans La Lettre Afnic #3).

- **Résolution 75 – Contribution du Secteur de la normalisation des télécommunications de l'UIT à la mise en œuvre des résultats du Sommet mondial sur la société de l'information, compte tenu du Programme de développement durable à l'horizon 2030**

  Cette résolution réaffirme l'importance du rôle de l'UIT dans la mise en œuvre des résultats du Sommet Mondial sur la Société de l'Information (SMSI), qui vise à réduire la fracture numérique et promouvoir un internet inclusif et collaboratif, et leur alignement avec les Objectifs de Développement Durable (ODD) des Nations Unies, au sein desquels les technologies jouent un rôle important dans l'éducation, la santé et la lutte contre le changement climatique.

  Bien que largement débattue, cette résolution n'a pas été modifiée vu les discussions stratégiques liées à la revue à 20 ans du SMSI prévue en 2025 et l'implémentation du Pacte numérique mondial voté en septembre 2024. La résolution souligne la nécessité de renforcer la collaboration internationale entre les États membres, les organisations internationales, le secteur privé et la société civile pour garantir un internet équitable et ouvert.

  Elle soutient également le modèle de gouvernance multipartite, déjà réaffirmé lors de l'événement NETmundial+10 au début de l'année 2024 et dans le Pacte numérique mondial (lire à ce sujet les articles *« NETmundial+10 : réaffirmer les principes d'une gouvernance d'internet multi-acteurs »* dans La Lettre Afnic #6 et *« Le Pacte Numérique Mondial a été adopté »* dans La Lettre Afnic #7).

  Par ailleurs, parmi les nombreuses thématiques abordées lors de cette Assemblée mondiale, certaines, bien qu'éloignées des problématiques spécifiques au DNS et à internet, reflètent des tendances majeures dans le secteur des télécommunications et des technologies émergentes. Certaines ont d'ailleurs fait l'objet de nouvelles résolutions.

- **Résolution 101 – Activités de normalisation du Secteur de la normalisation des télécommunications de l'UIT concernant les technologies fondées sur l'intelligence artificielle à l'appui des télécommunications/technologies de l'information et de la communication**

  Cette nouvelle résolution sur le sujet de l'intelligence artificielle (IA) donne instruction aux commissions d'études de l'UIT-T de continuer à travailler sur les applications de l'IA aux télécommunications/TIC dans la limite de leurs mandats. Elle mentionne une liste indicative de domaines, par exemple la fiabilité des télécommunications.

- **Résolution 105 – Promouvoir et renforcer la normalisation du métavers**

  Cette résolution, elle aussi nouvellement adoptée à New Delhi, s'intéresse au développement de normes internationales pour le métavers et le Web 4.0. Elle fait suite à la fin des travaux du *focus group* dédié au métavers. Elle vise à discuter l'interopérabilité, la sécurité et la durabilité de ces environnements numériques immersifs, tout en encourageant une collaboration internationale pour coordonner les efforts de normalisation.

Un pas de plus vers un internet véritablement universel

L'AMNT-24 s'est inscrite dans une continuité, réaffirmant les principes d'une gouvernance multipartite et inclusive pour relever les défis actuels et futurs des télécommunications et des infrastructures numériques. Les résolutions adoptées ou actualisées traduisent une ambition collective alors que la revue à 20 ans du SMSI se déroulera en 2025 et que la prochaine conférence de plénipotentiaires est prévue en 2026.

À l'aube d'une nouvelle étape dans la réflexion sur la gouvernance mondiale de l'internet, cet élan de coopération doit se prolonger, afin de s'assurer que les progrès technologiques continuent de bénéficier à tous, dans un esprit de durabilité et de solidarité mondiale.

03

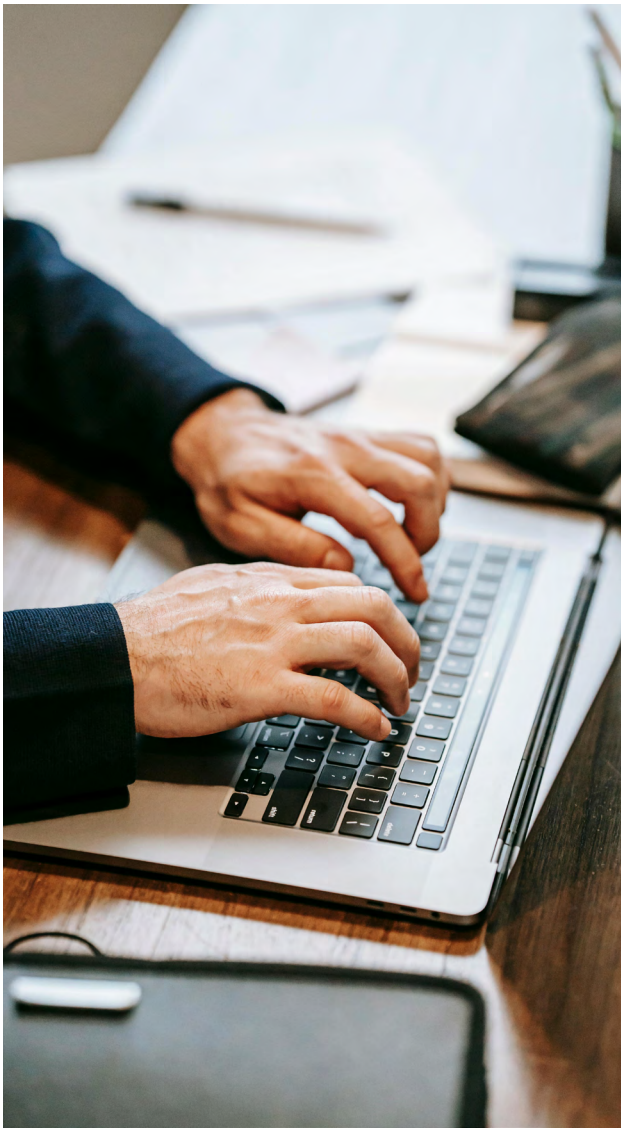
Le DNS, ça n'est pas que pour les sites web : zoom sur les enregistrements WALLET

Le DNS *(Domain Name System)* est bien plus qu'un simple traducteur de noms de domaine en adresses IP. Il est également capable de récupérer d'autres informations en réponse à une requête sur un nom de domaine, via un champ spécifique appelé *RR type* (*Resource Record type* ou type d'enregistrement) : ces enregistrements sont très variés, allant de ceux indiquant les serveurs de messagerie (enregistrements MX), à ceux décrivant des certificats de sécurité (enregistrements TLSA), des positions géographiques (enregistrements LOC), ou encore des informations textuelles libres (enregistrements TXT). Ils ne sont par ailleurs pas figés, de nouveaux pouvant être ajoutés au registre maintenu par l'IANA (*Internet Assigned Numbers Authority*, l'organisme chargé de la gestion des paramètres techniques d'internet) pour répondre à l'évolution des technologies et des usages numériques.

L'enregistrement WALLET : une nouvelle étape dans l'interopérabilité entre le DNS et la blockchain

Parmi les récents ajouts aux types qu'il est possible d'associer à un nom de domaine, l'enregistrement WALLET, qui a officiellement été intégré au registre IANA, démontre que le DNS peut efficacement répondre aux problématiques de résolution d'identifiants de l'écosystème de la blockchain et des cryptomonnaies.

Nous évoquions en effet dans La Lettre Afnic #7, plus précisément dans l'article *« DNS et systèmes de noms alternatifs : la nécessité d'une interopérabilité »*, les défis que soulève l'émergence de systèmes alternatifs au DNS, souvent basés sur des technologies telles que la blockchain. Ces systèmes, qui trouvent pour beaucoup leur origine dans l'écosystème des cryptomonnaies, cherchent à répondre aux mêmes besoins que ceux résolus dans l'internet : l'association entre « noms de domaine » – on parlera plutôt, en réalité, d'identifiants qui en ont l'apparence, car ils se situent en dehors du système DNS – et portefeuilles numériques basés sur la blockchain.



À quoi servent les enregistrements WALLET ?

Un enregistrement WALLET permet ainsi de tirer parti des capacités du DNS pour simplifier les transactions dans l'écosystème des cryptomonnaies. Il est constitué de deux champs : un identifiant indiquant la cryptomonnaie utilisée (par exemple, BTC pour Bitcoin ou ETH pour Ethereum) et une chaîne de caractères représentant l'adresse du portefeuille numérique.

En associant un nom de domaine familier à une adresse de portefeuille, il devient possible pour un utilisateur d'effectuer une transaction financière simplement en saisissant un domaine tel que « monentreprise.fr », évitant ainsi les erreurs fréquentes liées à la saisie de longues chaînes cryptographiques complexes.

Un enregistrement toujours en cours de normalisation

Bien que l'enregistrement WALLET soit officiellement enregistré auprès de l'IANA (sous le numéro 262), il reste en cours de normalisation. Actuellement défini dans le draft « DNS to Web3 Wallet Mapping », il fait toujours l'objet de discussions techniques à l'IETF, qui explorent les implications et les bonnes pratiques pour sa mise en œuvre, et ne bénéficie donc pas encore d'une RFC *(Request for Comments)* officielle.

Ces enregistrements sont par ailleurs encore peu pris en charge aujourd'hui : les serveurs DNS et les outils logiciels doivent être mis à jour pour intégrer ce type de manière native. En attendant, des solutions alternatives permettent aux administrateurs d'utiliser ces enregistrements dès maintenant, par le biais de mécanismes définis dans la RFC 3597, qui offrent un moyen d'associer des types non reconnus à un nom de domaine via une représentation brute.

L'interopérabilité entre le DNS et les systèmes alternatifs est essentielle pour maintenir la stabilité et l'universalité d'internet. Les standards à venir comme l'enregistrement WALLET pourraient servir de pont entre ces deux univers, en combinant la robustesse du DNS avec les innovations que peut apporter la blockchain.

4

L’application mobile France Identité a été reconnue conforme aux exigences de cybersécurité et d’interopérabilité du futur portefeuille d’identité numérique européen

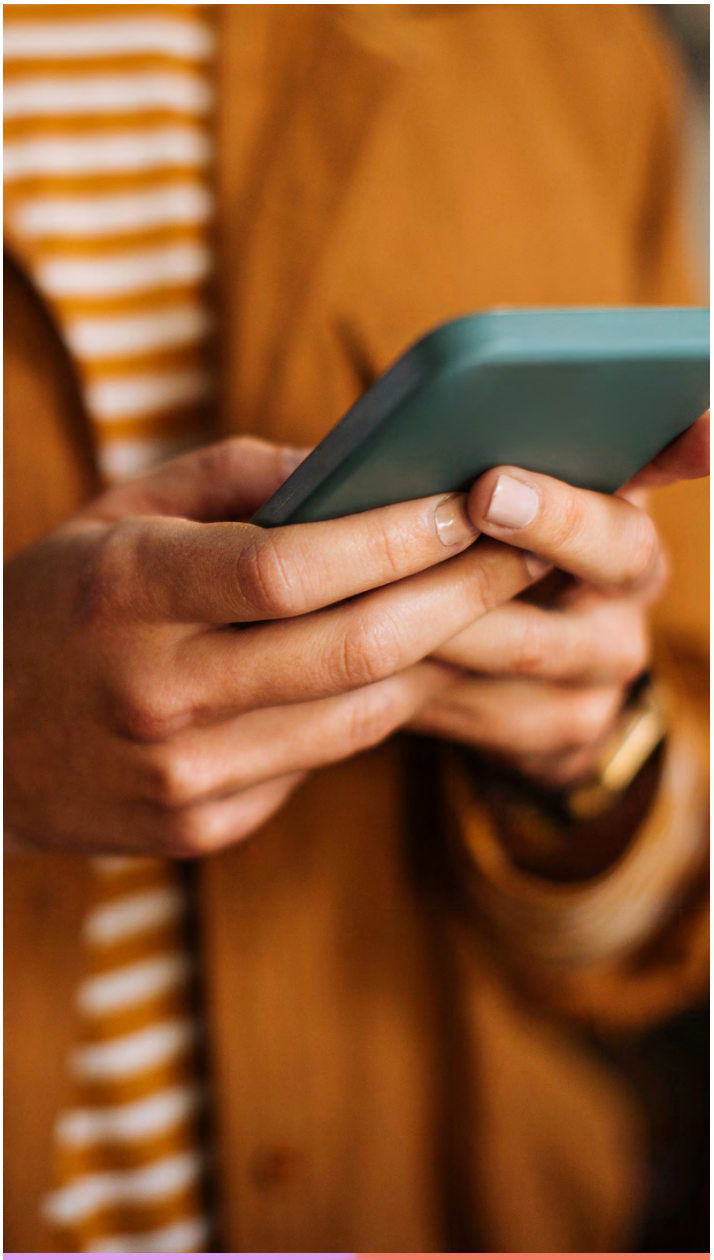
Fin 2023, la Commission européenne lançait un programme ambitieux visant à créer un portefeuille d'identité numérique européen d'ici 2026. L'objectif : permettre à tout résident, citoyen ou entreprise de l'Union européenne de stocker et prouver son identité en ligne de manière sécurisée, afin d'accéder à des services publics ou privés dans n'importe lequel des 27 États membres.

En France, plusieurs solutions d'identification numérique sont à disposition des utilisateurs pour accéder à leurs différents services sur internet. On retrouve parmi elles France Identité, une application mobile proposée gratuitement par le gouvernement français pour stocker les informations de la nouvelle carte nationale d'identité française, prouver son identité en ligne et simplifier l'accès aux démarches administratives.

En septembre dernier, France Identité a été reconnue, par la Commission européenne, conforme aux exigences relatives au niveau de garantie élevé dans le cadre du règlement européen eIDAS *(electronic Identification, Authentication and Trust Services)* sur l'identification électronique et les services de confiance. Cela signifie que France Identité répond aux normes les plus strictes fixées par l'Union européenne pour garantir un niveau élevé de sécurité et de fiabilité dans l'identification électronique, et qu'elle pourra, à terme, lorsque le portefeuille d'identité numérique européen sera effectivement déployé, être utilisée en toute confiance à travers l'Europe, de manière sécurisée et interopérable.

Cette reconnaissance souligne la participation active de la France dans la mise en œuvre du futur portefeuille d'identité numérique européen. En rejoignant d'autres pays, comme l'Allemagne ou l'Estonie, dont les solutions ont elles aussi été reconnues conformes aux exigences les plus élevées du règlement eIDAS, la France réitère sa volonté de contribuer à la création d'un écosystème numérique sécurisé et interopérable à l'échelle européenne.

C'est une étape importante qui, si elle marque l'avancement du programme, ne signe pas l'achèvement des travaux. Des questions restent en suspens et des problématiques à résoudre, comme nous le soulignions dans l'article *« Sécurité, interopérabilité et confiance sont les trois piliers du futur portefeuille d'identité numérique européen (EUDI) »* paru dans La Lettre Afnic #4. L'aboutissement du projet reposera sur la capacité de l'Europe à relever ces défis collectivement et à garantir une identité numérique qui inspire confiance à tous ses utilisateurs.



Les prochains événements auxquels l'Afnic participe :

- **30 janvier 2025**
  UIT Partner2Connect réunion annuelle 2024
  Genève, Suisse

- **6 et 7 février 2025**
  OARC 44
  Atlanta, États-Unis

- **10 et 11 février 2025**
  UIT Groupe de travail du Conseil sur le SMSI et les ODD
  Genève, Suisse

- **19 et 20 février 2025**
  UIT Groupe de travail du Conseil sur Internet
  Genève, Suisse

- **8 au 13 mars 2025**
  ICANN 82 Forum de la communauté
  Seattle, Etats-Unis

- **15 au 21 mars 2025**
  IETF 122
  Bangkok, Thaïlande

- **7 au 11 avril 2025**
  CSTD, 28e session
  Genève, Suisse

- **12 au 14 mai 2025**
  EuroDIG 2025
  Strasbourg, France

- **12 au 16 mai 2025**
  RIPE 90
  Lisbonne, Portugal

- **9 au 12 juin 2025**
  ICANN 83 Forum de politiques
  Prague, Tchéquie

- **17 au 27 juin 2025**
  Conseil de l'UIT
  Genève, Suisse

- **23 au 27 juin 2025**
  Forum sur la gouvernance de l'Internet 2025
  Lillestrøm, Norvège

- **7 au 11 juillet 2025**
  SMSI+20 Événement de haut niveau 2025
  Genève, Suisse

afnic
Internet made in France

Votre contact

lalettre@afnic.fr

Directeur de publication : Pierre Bonis

Afnic | www.afnic.fr
7 avenue du 8 Mai 1845,
78280 Guyancourt