La Lettre Afnic

n°4

Internet made in France

Bienvenue dans la quatrième édition de La Lettre Afnic. Cette publication trimestrielle, dédiée à la gouvernance technique de l'internet, a pour ambition de vous tenir informés des développements les plus récents, des enjeux stratégiques et des opportunités qui façonnent l'écosystème de l'internet en général, et de la gestion des noms de domaine en particulier. Nous espérons que sa lecture sera enrichissante et inspirante, nourrissant votre réflexion et votre vision de la gouvernance de l'internet.

Télécharger la version accessible

1

Sécurité, interopérabilité et confiance sont les trois piliers du futur portefeuille d'identité numérique européen (EUDI)

La question de l'identité numérique a récemment pris un nouveau tournant dans l'Union européenne. Le 9 novembre dernier, le Conseil et le Parlement européen sont en effet parvenus à un accord provisoire visant à instaurer un Portefeuille d'Identité Numérique Européen (EUDI) qui permettra de stocker son identité numérique de manière sécurisée et de réaliser diverses démarches administratives au sein de l'Union européenne avec son seul téléphone portable.

Ce portefeuille d'identité numérique offrira ainsi aux utilisateurs la possibilité de prouver leur identité via des attributs personnels (un permis de conduire, un compte bancaire, un diplôme, etc.) directement depuis leur smartphone. Il pourra être utilisé pour s'identifier sur les sites publics et privés dans les pays membres de l'Union européenne, tout en s'affranchissant des systèmes d'authentification tels que ceux des grands acteurs américains (Apple, Google, Meta, etc.).

Des étapes restent à parcourir avant l'approbation formelle du dispositif. Mais une fois le texte adopté, les pays membres de l'Union européenne disposeront de 24 mois pour le concrétiser et proposer à leurs citoyens des portefeuilles d'identité numérique. C'est un temps à la fois court et long, car des questions restent aujourd'hui encore en suspens concernant les technologies à utiliser et les défis à relever pour mettre en œuvre un portefeuille d'identité numérique à la fois efficace et sécurisé.

Identité, identifiant, moyen d'identification… de quoi parle-t-on ?

Une identité numérique se définit comme l'ensemble des informations et des données associées à un utilisateur sur internet. Elle englobe des éléments tels qu'une identité civile (nom, prénom, date de naissance…), des identifiants électroniques (pseudonymes, avatars…), des données de navigation (cookies), des commentaires, photos, vidéos publiés sur les réseaux sociaux, une adresse IP, une géolocalisation, etc.

Toutefois, au sens régalien qui nous intéresse ici, l'identité numérique regroupe les identifiants qui permettent à une personne de s'authentifier pour accéder à des services en ligne. Il peut s'agir de son état civil, mais également d'autres attributs personnels (son numéro de sécurité sociale, par exemple).

Un identifiant numérique est, quant à lui, une chaîne ou un ensemble de caractères qui permet d'identifier de manière unique une entité. Les identifiants sont couramment utilisés dans les systèmes d'authentification et d'autorisation pour permettre l'accès à des informations ou des services. L'usage d'identifiants permet de différencier les utilisateurs et de garantir un accès sécurisé aux systèmes et aux données, en évitant les conflits d'identité et en permettant une gestion individualisée des droits d'accès.

Un identifiant peut prendre différentes formes, telles qu'un nom d'utilisateur, une adresse email, un numéro d'identification unique, etc. À ce titre, l'adresse email fait partie des identifiants les plus répandus sur Terre : avec 4,3 milliards d'utilisateurs, c'est en effet plus de la moitié de la population mondiale qui l'utilise.

Un moyen d'identification numérique, enfin, est un outil, un dispositif ou un processus utilisé pour prouver ou vérifier l'identité de quelqu'un en ligne. Cela peut inclure des éléments tels qu'une application mobile, un mot de passe, une carte à puce, l'authentification par SMS ou encore la biométrie (identification faciale, empreinte digitale…).

Le moyen d'identification est ainsi l'instrument utilisé pour établir ou confirmer l'identité associée à un identifiant. Dans le cadre de l'accord provisoire du Conseil et du Parlement européen, le portefeuille d'identité numérique européen est un moyen d'identification numérique.

Quels sont les moyens d'identification numérique aujourd'hui disponibles ?

Il existe aujourd'hui en France différentes solutions d'identification numérique à disposition des utilisateurs pour se connecter à leurs différents services sur internet. Tous, néanmoins, ne sont pas interchangeables, visant des utilisateurs et/ou des services bien spécifiques. On retrouve notamment :

• **Les solutions d'identification des GAFAM** (et plus globalement, des grands acteurs américains de l'internet), qui sont intégrées à de nombreux sites internet et largement adoptées en France. Ces solutions, qui reposent sur les identifiants des comptes Google, Apple ID, Facebook Connect, etc., offrent aux utilisateurs la possibilité de s'authentifier de manière sécurisée sur une vaste gamme de services et de sites sur internet.

• **FranceConnect**, la solution d'authentification sécurisée proposée par l'Agence nationale des titres sécurisés (ANTS) en France. Sur un site qui dispose du bouton FranceConnect, elle permet aux utilisateurs de se connecter via un compte qu'ils possèdent déjà (au choix : un compte impots.gouv.fr, ameli.fr, l'Identité Numérique La Poste, msa.fr ou Yris).
Plus de 1 400 démarches relevant du service public – en relation avec la famille, la santé, la retraite, etc. – sont accessibles au travers de FranceConnect.

• **France Identité**, une application mobile officielle du gouvernement français, en test depuis 2022 et disponible gratuitement pour tous depuis septembre dernier. France Identité permet de stocker les informations présentes dans la nouvelle carte nationale d'identité pour prouver son identité en ligne et accéder plus facilement aux démarches administratives officielles. L'application fonctionne en lien avec FranceConnect et devrait, à terme, pouvoir également accueillir d'autres documents officiels dématérialisés comme le permis de conduire.

• **Les registres ccTLD**, également capables de fournir des identifiants. L'Afnic, par exemple, est devenu en 2021 membre d'ID4me, une association qui promeut un standard ouvert d'identité numérique décentralisée. Dans ce cadre, l'Afnic a développé et expérimenté une solution d'identité numérique pour les titulaires de noms de domaine en .fr, basée sur le système de noms de domaine et des protocoles ouverts OpenID Connect.

Les nouveaux identifiants numériques émergents

Les identifiants numériques émergents font référence à de nouvelles approches qui prônent une gestion décentralisée des identités numériques. Parmi les initiatives les plus visibles, on retrouve les DID (*Decentralized Identifiers*), portés par WC3 – le *World Wide Web Consortium*, une organisation internationale qui développe des normes pour le web afin d'assurer son évolution à long terme.

Les DID sont donc des identifiants numériques conçus pour être décentralisés — c'est-à-dire qu'ils ne dépendent pas d'une autorité centrale pour être émis ou validés. Au lieu de cela, ils sont étroitement liés à des environnements distribués — tels que la blockchain ou d'autres registres décentralisés. Dans ce contexte, les DID apportent aux utilisateurs un contrôle plus direct sur leurs identités : ils peuvent décider quelles informations partager, avec qui et quand, tout en conservant la propriété de leurs données personnelles. Les informations d'identité sont stockées de manière sécurisée car la technologie, robuste, offre des caractéristiques de cryptographie avancée et d'immutabilité des données qui renforcent la cybersécurité des identifiants numériques.

Les DID sont souvent mis en œuvre sur des blockchains pour tirer parti de la sécurité et de la décentralisation qu'offre cette technologie. Chaque DID peut y être enregistré de manière immuable, fournissant ainsi un historique transparent des transactions et des changements d'état associés à l'identité numérique. Mais la blockchain n'est pas la seule technologie distribuée permettant d'assurer la sécurité et l'intégrité des identifiants, et de renforcer la confiance dans les transactions numériques et les interactions en ligne. L'écosystème DNS présente également de nombreux atouts.

Les DID et l'écosystème DNS

S'ils offrent l'avantage d'être à la fois décentralisés et sécurisés, les DID ne sont pas sans défaut. Ils sont difficiles à mémoriser, car leur structure est complexe, composée d'une longue chaîne de caractères hexadécimaux, et leur format est non conventionnel. Ils doivent par ailleurs être intégrés à des systèmes déjà existants, ce qui peut poser des problèmes d'interopérabilité, notamment lorsqu'ils reposent sur la blockchain car la technologie n'est pas encore largement adoptée.

Pour surmonter ces défis, des approches telles que la publication des DID dans le DNS (*Domain Name System*) peuvent être envisagées. En utilisant le DNS, les DID peuvent être associés à des noms de domaine familiers via des enregistrements DNS (tout comme le sont déjà

les adresses IP), simplifiant ainsi leur découverte et leur utilisation. Et le DNS étant une technologie largement adoptée et utilisée sur internet, l'intégration des DID dans le DNS va pouvoir profiter de l'infrastructure existante et améliorer l'interopérabilité et la confiance dans les échanges d'informations d'identification.

Cette approche fait l'objet de plusieurs travaux expérimentaux et marques d'intérêt, notamment :

• En 2021 déjà, l'IETF publiait un draft, aujourd'hui expiré, faisant état de travaux expérimentaux, proposant une méthode standardisée fonctionnelle pour associer des DID à des noms d'hôtes et à des adresses email, facilitant ainsi la découverte de ces identifiants décentralisés dans l'écosystème DNS.

• Plus récemment, CIRA, le Registre de noms de domaine canadien, a présenté lors de réunions ICANN « DID to DNS with DNSSEC » (DID vers DNS avec DNSSEC), explorant la connexion entre les identifiants décentralisés et le DNS/DNSSEC, ou encore « The Challenge of Using 'the' DNS in 'a' Digital Credential World » (Le défi d'utiliser « le » DNS dans « un » monde d'identifiants numériques).

Une question de confiance

De même, si les DID apportent une couche de sécurité à la gestion des informations d'identité, reste la question de la confiance. Comment s'assurer, en effet, que les informations d'identité gérées par les systèmes tels que les DID sont fiables et crédibles ? La confiance concerne ainsi la certitude que les informations d'identité présentées ou utilisées sont non seulement authentiques et non altérées, mais aussi émises par des entités légitimes.

Ici encore, le DNS, associé à DNSSEC (*DNS Security Extensions*) – une extension du DNS visant à renforcer la sécurité du système de noms de domaine –, peut jouer un rôle essentiel permettant d'établir cette confiance. L'émission d'identifiants numériques est souvent gérée par des émetteurs spécifiques, et ces informations peuvent être enregistrées dans le DNS, via des enregistrements TLSA (*Transport Layer Security Authentication* – un type d'enregistrement DNS utilisé pour spécifier des informations d'authentification associées à un service sécurisé), signés et validés avec DNSSEC.

En signant numériquement les enregistrements DNS, DNSSEC garantit l'authenticité des informations et protège contre les modifications malveillantes. Ainsi, lorsqu'un utilisateur présente une identité numérique intégrant des informations vérifiables, comme une preuve numérique de son âge ou de la validité de son permis de conduire, la vérification cryptographique via DNSSEC assure l'intégrité des données liées aux DID.

Quels sont aujourd'hui les projets et initiatives en cours pour promouvoir l'identité numérique ?

L'accord provisoire sur la mise en place d'un portefeuille d'identité numérique européen est l'un des projets les plus importants. Nous avons déjà abordé le sujet en introduction, mais certains détails méritent encore d'être soulignés :

• Dans le texte de la proposition de règlement, la révision de l'article 45 en particulier soulève des inquiétudes. Elle vise en effet à modifier la gestion des certificats de sécurité – c'est-à-dire des fichiers électroniques assurant la sécurité des échanges de données entre un navigateur web et un serveur –, obligeant les éditeurs à choisir parmi des émetteurs validés uniquement par les États membres de l'Union européenne. Les experts craignent que cette mesure puisse potentiellement ouvrir la porte à une surveillance généralisée du trafic internet des citoyens européens, en dépit du respect de la vie privée des utilisateurs.

• D'autres préoccupations concernent le risque de centralisation excessive de données entre les mains des États et le manque de transparence dans le processus décisionnel.

• Du côté des utilisateurs, des craintes existent également quant à la possible imposition d'une identification obligatoire en ligne, bien que le texte propose des garanties, telles que le droit à la pseudonymisation et la minimisation des données.

Les signataires d'une lettre ouverte, parmi lesquels figurent de grandes organisations telles que Cloudflare, la fondation Linux et Mozilla, appellent à une révision attentive de cette proposition, mettant en garde contre les conséquences sur la souveraineté numérique et les libertés fondamentales des citoyens de l'Union européenne.

La Commission européenne a, quant à elle, investi 46 millions d'euros dans quatre projets pilotes pour développer le portefeuille d'identité numérique européen dans le cadre du programme pour une Europe numérique. Ces projets, qui bénéficient d'un investissement total de plus de 90 millions d'euros, couvrent un large éventail de cas d'utilisation, allant des services publics et privés aux interactions nationales et transfrontalières. Coordonnées par différents pays, dont la France, l'Allemagne, la Suède et la Norvège, ces initiatives testeront le portefeuille EUDI dans des domaines variés tels que l'accès aux services publics, l'ouverture de comptes bancaires, la gestion des paiements, la mobilité avec le permis de conduire mobile, la signature électronique, la gestion des données médicales… Les projets impliquent plus de 250 organisations, dont des registres de noms de domaine, dans presque tous les États membres, mettant l'accent sur l'amélioration de l'accès des citoyens à des moyens d'identité électronique fiables et sécurisés.

La dernière réunion IETF118, qui s'est déroulée à Prague en novembre dernier, a également été le lieu de nombreux échanges et discussions sur les identités et identifiants numériques, impliquant des acteurs majeurs tels que l'Union européenne, l'Internet Engineering Task Force (IETF) et le World Wide Web Consortium (W3C), et reflétant la complexité de l'écosystème des solutions d'identité numérique. Avec la diversité croissante des approches et des socles techniques déployés ou envisagés, il devient impératif de renforcer les liaisons entre ces initiatives, au risque sinon de fragmenter l'écosystème. Les experts, conscients des enjeux, soulignent l'importance d'une coordination renforcée pour garantir une intégration harmonieuse des solutions et assurer une expérience utilisateur transparente. Notons en particulier, lors de cet IETF118, la présentation du groupe de travail SPICE (*Secure Patterns for Internet CrEdentials* – modèles sécurisés pour les identifiants sur internet) qui souligne l'importance de concevoir soigneusement les identifiants, y compris les DID, pour garantir la confidentialité et la sécurité.

En conclusion

La question de la gestion des identités numériques évolue rapidement. Les projets européens, les débats à l'IETF, les investissements dans le développement de solutions témoignent à la fois de la complexité du débat et de l'enthousiasme de ses parties prenantes.

Mais que l'on s'intéresse aux projets de règlementation au niveau européen ou aux initiatives lancées individuellement ou collectivement par la communauté technique, il est nécessaire de comprendre et de prendre en compte la diversité des solutions d'identification numérique et la façon dont elles peuvent fonctionner ensemble. Car si l'on peut percevoir le fait qu'un seul utilisateur puisse avoir des dizaines, voire des centaines d'identifiants comme un avantage pour contrer la centralisation des fournisseurs et des données, la complexité de leur gestion à long terme peut également poser problème.

C'est dans l'interopérabilité, la sécurité et la confiance dans les systèmes que réside la clé de voûte de l'écosystème. Et en la matière, l'intégration des identifiants émergents au sein de l'infrastructure DNS existante suscite un intérêt. Plus loin encore, les registres de noms de domaines pourraient jouer un rôle essentiel en devenant des autorités parties-prenantes de solutions d'identification, qu'elles soient d'initiative publique ou privée.

2

Zoom sur les bureaux d'enregistrement de noms de domaine : qui sont-ils, que font-ils ?

Beaucoup de registres de noms de domaine ne vendent pas les noms en direct. Par exemple, pour enregistrer un nom de domaine en .fr ou l'une des 18 autres extensions gérées par l'Afnic, il faut passer par un bureau d'enregistrement. C'est également vrai pour de nombreux autres TLD (*Top Level Domain*), à l'instar du .com géré par Verisign.

Les bureaux d'enregistrement (BE) jouent ainsi un rôle central dans l'écosystème du DNS. Ils sont des intermédiaires en lien contractuel avec les registres, autorisés à proposer des services d'enregistrement de noms de domaine aux titulaires potentiels. Les BE agissent en tant que guichet unique, permettant aux organisations, entreprises et particuliers d'acquérir et de gérer leurs noms de domaine.

Les bureaux d'enregistrement sur le devant de la scène avec NIS 2

2024 s'annonce comme une année charnière pour les bureaux d'enregistrement, car elle marquera l'entrée en vigueur de la directive NIS 2, visant à renforcer la cybersécurité dans l'Union européenne. Cette évolution réglementaire pourrait avoir un impact significatif sur le mode de fonctionnement des bureaux d'enregistrement dans la gestion des noms de domaine et leur conformité à de nouvelles exigences en matière de cybersécurité.

NIS 2 fait en effet suite à NIS 1, la directive *Network and Information Security* adoptée par le Parlement et le Conseil de l'Union européenne en 2016 face à la rapide montée en puissance des cybermenaces. NIS 1 avait pour objectif principal de renforcer la cybersécurité en imposant des obligations aux acteurs clés de secteurs dits « essentiels », comme les fournisseurs d'énergie, les établissements de santé, les institutions financières ou les opérateurs de réseaux de télécommunications.

Depuis, les acteurs malveillants ont gagné en sophistication et les vulnérabilités touchent aujourd'hui un nombre croissant d'entreprises et d'organisations toujours plus interconnectées. Cette réalité soulève un nouvel enjeu : il ne suffit plus que les acteurs essentiels soient bien protégés pour garantir leur cybersécurité.

Les risques ne se limitent pas à leur seul périmètre, mais s'étendent également à leurs fournisseurs. C'est de la cybersécurité de chaque maillon que dépend la robustesse de l'ensemble de l'écosystème.

C'est dans ce contexte que NIS 2 s'impose comme une avancée majeure. La directive, qui devrait entrer en vigueur au plus tard en octobre 2024 en France, repose sur les acquis de NIS 1 tout en s'étendant bien au-delà. Elle élargit en effet considérablement son champ d'application en ne se limitant plus seulement aux opérateurs de services essentiels, mais aussi à leurs fournisseurs de services numériques, à leur chaîne d'approvisionnement critique, ainsi qu'aux administrations publiques.

Parmi les acteurs nouvellement inclus, on trouve les bureaux d'enregistrement, désignés explicitement comme relevant de NIS 2 dans les textes de la directive pour ce qui relève de leur rôle de collecte de données des titulaires de noms (article 28). Il faut dire qu'ils jouent un rôle central dans la gestion des noms de domaine.

Quel est le rôle exact des bureaux d'enregistrement ?

Les missions des bureaux d'enregistrement sont multiples, au confluent des services aux utilisateurs finaux, des règles émises par les registres et des exigences réglementaires.

Dans sa relation avec les titulaires, la mission principale d'un BE est de leur permettre d'enregistrer des noms de domaine. Cela inclut la vérification de la disponibilité du nom de domaine souhaité, la gestion du processus d'enregistrement et l'assistance à l'utilisateur tout au long du processus. Une fois le nom de domaine enregistré, les BE assurent également sa gestion continue : renouvellements, éventuels transferts, résolution de problèmes techniques liés au nom de domaine, etc.

Les BE doivent également respecter les politiques et les règles établies par le registre en matière d'enregistrement et de gestion des noms de domaine. Cela garantit que les noms de domaine sont attribués conformément aux normes établies. Les critères d'accréditation de l'Afnic, par exemple, s'inscrivent dans les dispositions du Code des Postes et des Communications Électroniques et incluent la maîtrise des aspects techniques, la vérification des données d'identification, les ressources humaines et techniques nécessaires, la sécurité des données personnelles et des conditions d'accueil du public adéquates.

Il revient également aux BE de renseigner et mettre à jour les informations de la base de données des titulaires, qui constituent une base de données internationale et publique sur les noms de domaine, incluant les noms des titulaires, les contacts administratifs, techniques et de facturation, etc. Elle permet à tout un chacun d'obtenir des informations sur les noms de domaine, notamment leur disponibilité, leur titulaire (s'il n'est pas anonymisé) et leurs serveurs de noms associés. Le registre peut utiliser ces informations pour faciliter la communication avec les titulaires et autres besoins liés à la gestion des noms de domaine.

Fun facts

Le réseau du .fr compte 400 bureaux d'enregistrement accrédités. Pour la majorité d'entre eux, l'enregistrement de noms de domaine n'est pas leur activité principale. On y trouve une grande variété d'entreprises telles que des hébergeurs web, des fournisseurs d'accès à internet, des agences web, communication, marketing ou e-commerce, des fournisseurs de services informatiques...

Les 3 plus gros BE accrédités par l'Afnic gèrent 60 % des noms de domaine en .fr. Cette concentration s'explique par la diversité des profils des bureaux d'enregistrement accrédités. Nombre d'entre eux ne gèrent qu'un nombre restreint de noms de domaine.

Il n'est pas nécessaire d'être installé en France pour devenir un bureau d'enregistrement accrédité de l'Afnic. Il est toutefois impératif de respecter les règles et les critères d'accréditation établis par l'Afnic. Parmi ces règles, on retrouve notamment la restriction selon laquelle les noms de domaine en .fr ne peuvent être utilisés que par des titulaires établis au sein de l'Union européenne.

Des missions intrinsèquement liées à la cybersécurité et à la prévention des abus sur internet

Le rôle des BE ne se limite pas à faciliter l'enregistrement et la gestion des noms de domaine en accord avec les directives de leur registre. Ils participent également à la cybersécurité et contribuent à la lutte contre les abus sur internet.

Les BE assument en effet la responsabilité de la collecte des informations personnelles des utilisateurs lors de l'enregistrement de noms de domaine. À ce titre, ils doivent mettre en place des mesures de protection robustes pour garantir que ces données sont collectées, stockées et traitées en conformité avec les réglementations en matière de protection des données, telles que le Règlement Général sur la Protection des Données (RGPD) en Europe. Leur rôle est donc aussi de veiller à ce que les informations des utilisateurs soient correctement protégées et ne soient pas exposées publiquement. Ce faisant, ils contribuent à maintenir la sécurité, la confidentialité et l'intégrité des données personnelles au sein de l'écosystème DNS.

Les missions des BE permettent également de lutter contre les abus sur internet. La vérification des informations d'identification des propriétaires de noms de domaine contribue en effet à la traçabilité des acteurs impliqués dans des activités en ligne illégales. Les BE peuvent collaborer avec les forces de l'ordre pour enquêter sur des cas d'abus et fournir des informations sur les propriétaires de noms de domaine, les enregistrements DNS, etc., pour aider à identifier et poursuivre les criminels.

En fin de compte, les bureaux d'enregistrement de noms de domaine sont des acteurs clés dans la préservation de l'intégrité et de la sécurité d'internet. Ils travaillent en collaboration avec d'autres parties prenantes, telles que les registres de domaines, les fournisseurs d'hébergement, les forces de l'ordre et les organisations de défense des droits numériques, pour s'attaquer aux abus en ligne et maintenir un environnement en ligne plus sûr.

Bureau d'enregistrement, revendeur, proxy : savez-vous à qui vous avez vraiment affaire ?

Lorsqu'un utilisateur décide d'acquérir un nom de domaine, il est important qu'il comprenne les différents acteurs qui peuvent être impliqués dans ce processus. Car si les bureaux d'enregistrement sont les seuls à pouvoir enregistrer officiellement le nom de domaine auprès du registre, la demande initiale peut tout aussi bien être passée auprès d'un revendeur de noms de domaine ou d'un service de proxy.

Bureau d'enregistrement
Un bureau d'enregistrement est une entité autorisée par les registres, telles que l'Afnic pour le .fr, à enregistrer des noms de domaine auprès d'eux. Les bureaux d'enregistrement interagissent directement avec les registres et sont responsables de la collecte et de la vérification des informations d'identification des propriétaires de noms de domaine conformément aux réglementations en vigueur.

Revendeur de noms de domaine
Un revendeur de noms de domaine est une entité qui agit en tant qu'intermédiaire entre les bureaux d'enregistrement et les titulaires de noms de domaine. Il agit pour le compte de ses clients en gérant le dépôt et le renouvellement de leurs noms de domaine auprès des bureaux d'enregistrements. On retrouve, par exemple, parmi les revendeurs des agences web ou de référencement, mais aussi des conseils en propriété intellectuelle.

Service de proxy
Un proxy propose de s'identifier comme le titulaire d'un nom de domaine en lieu et place de son client – le vrai titulaire. Un utilisateur peut y faire appel lorsqu'il ne souhaite pas voir apparaître ses données personnelles, offrant ainsi un certain degré d'anonymat. Le proxy porte alors la responsabilité légale du nom de domaine de son client.

Sous .fr, l'offre d'anonymisation par proxy n'est pas nécessaire, elle est d'ailleurs assez peu développée. Et pour cause, le .fr a été la première extension de premier niveau à restreindre la publication des données personnelles des personnes physiques titulaires de noms de domaine. Cela n'empêche pas l'Afnic de lever l'anonymat quand une demande d'accès à ces informations est effectuée par une personne, morale ou physique, ayant un intérêt à agir.

Il est à noter que l'ajout d'intermédiaires ou de prestataires tels que les revendeurs et les services de proxy peut compliquer la traçabilité en cas d'abus sur Internet. Par exemple, les bureaux d'enregistrement ont la responsabilité de collecter et vérifier les informations, là où les services de proxy peuvent rendre plus complexe l'identification des propriétaires en cas de problème.

3

Universal Acceptance : les défis d'un internet linguistiquement inclusif

L'*Universal Acceptance* (UA), ou acceptance universelle en français, est l'un des piliers d'un internet véritablement mondial et inclusif, où chaque individu, quelle que soit sa localisation, le choix d'extension internet qu'il opère (.fr, .com, .paris…) ou sa langue maternelle, peut accéder à l'ensemble des services de l'écosystème numérique.

Selon le principe de l'UA, chaque identifiant en ligne, qu'il s'agisse d'un nom de domaine ou d'une adresse email, doit en effet pouvoir être compris et traité de manière équitable et transparente par l'ensemble des infrastructures numériques. L'objectif premier est de transcender les barrières linguistiques, culturelles et d'écriture, en permettant l'utilisation de toutes les formes d'identifiants, indépendamment de leur origine géographique ou de leur alphabet, partout en ligne, pour peu que ces identifiants respectent les règles et standards mis en place par l'IETF[1] et l'ICANN[2].

Noms de domaines et adresses emails internationalisés

C'est au début des années 2000 que l'on a pu voir apparaître les premiers noms de domaine internationalisés (IDN). Les noms de domaine étaient auparavant limités aux caractères ASCII[3] standard, principalement alphabétiques latins ; l'introduction des IDN a permis d'enregistrer des noms de domaine utilisant des caractères issus de divers alphabets, tels que l'arabe, le chinois, le cyrillique, etc. L'internationalisation des adresses email (EAI) a suivi, permettant l'utilisation de caractères spéciaux et internationaux dans les adresses email. Cette évolution s'est faite un peu avant l'ouverture par l'ICANN de nouvelles extensions génériques, ajoutant un millier de nouvelles extensions de noms de domaines de premier niveau dans la racine d'internet. L'ensemble de ces nouveaux identifiants entraîne depuis plusieurs années la nécessité qu'ils soient reconnus et acceptés par tous les intervenants et acteurs des services numériques.

Dans ce contexte, l'Universal Acceptance permet de garantir que les noms de domaine comme « 例子.com » (où les caractères chinois signifient « exemple »), « مثال.شبكة » (où « مثال » signifie « exemple » en arabe et « شبكة. » est l'extension de domaine signifiant « réseau » en arabe), ou avec une extension en .рф (l'extension russe en cyrillique) sont correctement traités partout en ligne, permettant aux utilisateurs d'accéder à des sites web dans leur langue, quelle qu'elle soit, tout en préservant la spécificité de leur écriture. De la même manière, une adresse email telle que « prénom@café.fr » avec des caractères spéciaux (des accents) à la fois dans l'identifiant « prénom » et dans le domaine de messagerie « café.fr », devrait être acceptée sans problème selon les principes de l'UA.

En théorie. Car la réalité est tout autre. Aujourd'hui encore, lorsqu'un nom de domaine, une extension ou une adresse email comporte des caractères autres que les ASCII standard, voire quand il s'agit d'une nouvelle extension insérée récemment dans la racine, telle que .music par exemple, des problèmes peuvent être rencontrés à plusieurs niveaux : certains navigateurs, applications ou systèmes d'exploitation ne prennent toujours pas en charge correctement leur affichage ; de nombreux formulaires en ligne ne reconnaissent pas les adresses email internationalisées ; certains systèmes de sécurité, comme des filtres anti-spam, ne sont pas

1. L'IETF, ou *Internet Engineering Task Force*, est un organisme international impliqué dans le développement et la normalisation des protocoles internet.
2. L'ICANN, ou *Internet Corporation for Assigned Names and Numbers*, est une organisation internationale chargée de coordonner et de superviser les aspects techniques et opérationnels des systèmes de noms de domaine et des adresses IP sur internet.
3. L'ASCII, ou *American Standard Code for Information Interchange*, est une norme informatique d'encodage de caractères. Elle contient 128 caractères codés sur 7 bits : les chiffres arabes de 0 à 9, les 26 lettres de l'alphabet latin en minuscules et en capitales, des symboles mathématiques et de ponctuation.

configurés pour gérer correctement les caractères non latins, empêchant l'émission ou la bonne délivrabilité des emails concernés. Enfin, certains formulaires ou filtres non mis à jour rejettent les extensions internet qu'ils ne connaissent pas, alors même que ces dernières ont été acceptées au niveau international et des protocoles, et insérées dans la racine du système des noms de domaine.

Le rapport en demi-teinte de l'UASG

La mise en œuvre de l'Universal Acceptance s'est ainsi rapidement révélée être un défi complexe. C'est pour le relever qu'a été fondé en 2015 l'Universal Acceptance Steering Group (UASG), un groupe de travail international composé de plus de 500 membres bénévoles, issus d'une multitude d'entreprises, gouvernements et organisations dans le secteur de l'internet, et qui s'efforce de promouvoir l'Universal Acceptance.

Parmi ses travaux, l'UASG réalise des études et des mesures de l'UA, afin d'identifier et de résoudre les problèmes techniques qui y sont liés, et d'évaluer la progression de son adoption par toutes les parties prenantes de l'internet.

Selon l'édition 2023 de son Rapport sur l'état de préparation à l'acceptation universelle, réalisé en collaboration avec l'ICANN *(Internet Corporation for Assigned Names and Numbers)*, deux niveaux sont à prendre en compte pour l'UA : les outils de développement utilisés pour créer des solutions numériques d'une part, et les applications logicielles effectivement utilisées par les utilisateurs finaux d'autre part (applications mobiles, sites web, services de messagerie, etc.).

En effet, il ne suffit pas d'utiliser des technologies prenant en compte l'Universal Acceptance pour développer des solutions prêtes pour l'UA. Chaque étape de conception, développement et déploiement des applications logicielles doit intégrer le principe d'UA pour que cela puisse fonctionner. À chacune de ces couches, cela signifie la prise en charge des noms de domaine, y compris les IDN, et des adresses électroniques, y compris les EAI. Ajoutez-y la multitude d'alphabets dans le monde, les sens d'écriture, les jeux de caractères… et les complications émergent.

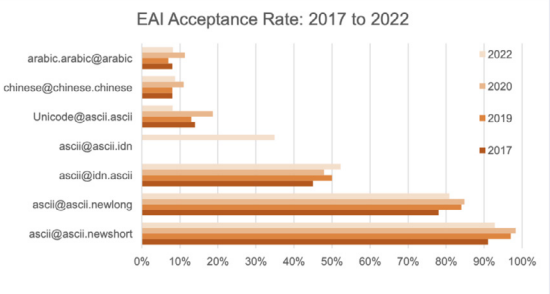
C'est probablement ce qui explique que les mesures effectuées par l'UASG pour évaluer le niveau d'adoption de l'UA au sein des plateformes techniques (langages de programmation, outils d'hébergement web…), des applications (navigateurs, médias sociaux…), des logiciels et services de messagerie, montrent que la bataille est loin d'être gagnée.

Un exemple est particulièrement criant : celui de l'évolution de l'acceptation de différents types d'adresses email par les sites web, qui stagne voire régresse au fil des ans (voir notre encadré).

Taux d'acceptation des emails de 1 000 sites web mondiaux et de 1 000 sites web nationaux

Dans le Rapport sur l'état de préparation à l'acceptation universelle de l'UASG et de l'ICANN, l'une des mesures suivies illustre parfaitement la situation de l'UA en 2023 : celle du taux d'acceptation des adresses email par une liste représentative de sites web globaux et locaux.

Depuis 2017, l'UASG a en effet mené plusieurs fois la même étude pour vérifier les taux d'acceptation par les sites web de différents types d'adresses email, en testant une variété d'extensions y compris les IDN, ainsi que des identifiants pouvant comporter des caractères non ASCII.



(Source)

Ce schéma montre clairement des niveaux d'acceptation similaires au fil des années, ce qui suggère que les développeurs n'améliorent pas leurs sites web pour intégrer les fonctionnalités liées à l'UA. De façon préoccupante, on peut constater une régression entre les résultats de 2020 et ceux de 2022, sur quasiment toutes les variantes testées.

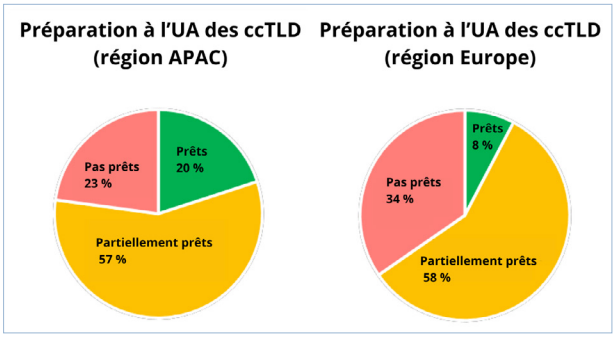
Le rôle des ccTLD dans la promotion de l'UA au niveau national

Dans son livre blanc The Role of ccTLDs in Achieving Universal Acceptance (Le rôle des ccTLD dans l'adoption de l'Universal Acceptance), l'association des noms de domaine de premier niveau d'Asie-Pacifique (APTLD) insiste sur l'important rôle des ccTLD (pour *country code top-level domain* ou domaine de premier niveau national, c'est-à-dire les extensions nationales telles que le .fr pour la France ou le .ca pour la Canada), dans la promotion de l'UA au niveau national.

Selon l'APTLD, qui regroupe nombre de membres ayant l'usage quotidien d'alphabets non latins et qui est donc en première ligne sur ce sujet, les ccTLD peuvent susciter une prise de conscience, mettre en place des formations et des actions de sensibilisation, adopter eux-mêmes l'UA comme modèle, fournir un soutien technique et aider à coordonner les efforts liés à l'UA avec d'autres organisations publiques et privées et d'autres influenceurs.

À leur sujet, l'enquête « Universal Acceptance (UA) – Readiness Survey Report – ccTLDs » (Universal Acceptance – Rapport d'enquête sur la préparation des ccTLD), réalisée par l'ICANN début 2023, montre une tendance plutôt positive. D'après les résultats de cette enquête, 69 % des ccTLD se déclarent prêts (13 %) ou partiellement prêts (56 %) pour l'UA. Parmi les ccTLD qui ne sont pas totalement prêts pour l'UA, 31 % l'ont incluse dans leur feuille de route et 50 % prévoient de commencer à travailler dessus dans les 12 prochains mois. Ils déclarent le faire tout à la fois pour des raisons commerciales (améliorer la qualité de leur service, répondre aux attentes de leurs clients, accroître la base d'utilisateurs…), et pour soutenir les communautés linguistiques locales.

On note toutefois des différences entre les grandes régions du monde, comme l'illustre ce schéma tiré de l'enquête de l'ICANN : le taux de préparation à l'UA parmi les ccTLD de la région Asie Pacifique (APAC) est plus élevé que celui des ccTLD de la région Europe.



(Source)

Il faut dire que la région APAC est extrêmement diversifiée sur le plan linguistique. Nombreux sont les pays asiatiques utilisant des scripts et des alphabets différents. Cette diversité linguistique constitue un défi stimulant et, simultanément, une opportunité inestimable, poussant naturellement la région à œuvrer en faveur de l'UA.

Un indispensable travail de sensibilisation à tous les niveaux

Pour aller plus loin, lors du dernier ICANN78 qui s'est déroulé en octobre dernier, l'UASG a présenté une liste des initiatives locales en faveur de l'Universal Acceptance, c'est-à-dire des initiatives visant à impliquer les parties prenantes locales dans le déploiement de l'UA, tout en menant des actions de sensibilisation et de formation au niveau national.

Force est de constater que le continent asiatique s'y démarque à nouveau, totalisant 4 des 5 initiatives listées : en Chine (par l'Internet Society of China), en Inde (par la FICCI-ILIA – Alliance internet en langue indienne), au Sri Lanka (via Theekshana), en Thaïlande (via le THNIC – Thai Network Information Center). La dernière initiative présentée étant, quant à elle, menée par des registres IDN TLD et entreprises IT de 7 pays de la CEI-EE (Communauté des États indépendants et Europe de l'Est).

L'UASG et l'ICANN œuvrent par ailleurs à la diversité géographique des initiatives, notamment auprès des régions Amérique latine et Europe, et poursuivent leurs travaux d'influence et de mobilisation pour multiplier les actions en faveur de l'UA partout dans le monde.

Embarquer les géants de l'internet

C'est dans cet esprit que l'UASG et l'ICANN déploient notamment d'importants efforts pour influencer les géants de l'internet, sensibilisant des entreprises telles que Meta ou WordPress et les incitant à adopter des pratiques exemplaires en matière d'Universal Acceptance.

Lors de la réunion ICANN77 (en juin 2023), l'ICANN avait ainsi préparé une liste de problèmes concrets et Meta avait envoyé un représentant capable d'identifier l'équipe appropriée pour chacun d'entre eux. Depuis, Meta a résolu le problème de blocage sur Facebook de liens vers certains noms de domaine internationalisés (IDN) tels que café.fr ; d'autres problèmes identifiés sont par ailleurs actuellement traités par les équipes de Meta, qui devraient prochainement leur apporter une solution.

Une journée de mobilisation en faveur de l'UA

Par ailleurs, l'UASG, en collaboration avec l'ICANN, a lancé en 2023 le tout premier UA Day, un événement visant à mobiliser des parties prenantes locales, régionales et mondiales pour sensibiliser et encourager l'adoption de l'UA. Ce jour, qui combine des sessions informatives et formatrices virtuelles, en personne et hybrides, a été créé pour unir les communautés techniques et linguistiques, les entreprises, les gouvernements et les acteurs du DNS afin de promouvoir l'UA et un internet multilingue à l'échelle mondiale.

L'UA Day ne se contente par ailleurs pas d'être un événement informatif ; c'est également une opportunité pour la communauté mondiale de contribuer activement à la cause de l'UA. L'appel à propositions pour l'UA Day 2024, qui se tiendra le 28 mars prochain, est actuellement ouvert, invitant toutes les organisations et professionnels à soumettre des propositions d'événements. Cette participation active est cruciale, car elle permet de partager des idées novatrices, de discuter des défis actuels liés à l'UA et de collaborer pour trouver des solutions concrètes.

Les défis actuels sont nombreux, mais présagent d'un avenir prometteur où les barrières linguistiques et les risques de fragmentation liés pourront enfin s'estomper sur internet. Grâce aux avancées technologiques, à toujours plus de sensibilisation et à l'engagement continu de toutes les parties prenantes, l'écosystème numérique évoluera vers toujours plus d'inclusivité et d'universalité.

Mais ce que nous dit aussi cette bataille pour l'acceptation universelle des identifiants, c'est la complexité de l'écosystème numérique mondial où des acteurs, du plus petit au plus gros, peuvent, s'ils ne suivent pas les recommandations issues des protocoles et règles établis dans les enceintes de gouvernance de l'internet, fortement retarder leur déploiement. Aucune règle, et cela s'applique également aux régulations et aux lois, ne peut se déployer sur internet par la seule vertu de son édiction. Associer l'ensemble des acteurs concernés à l'élaboration de ces règles est donc une nécessité opérationnelle, qui probablement n'a pas été totalement prise en compte au moment de l'élaboration des IDN et du lancement des nouvelles extensions. Cette leçon, qui va dans le sens d'un renforcement du modèle multi-acteurs, est essentielle.

Les prochains événements auxquels l'Afnic participe

22 janvier au 2 février 2024
Réunions des groupes de travail du Conseil et des groupes d'experts de l'UIT
Genève, Suisse

8 et 9 février 2024
DNS-OARC 42 (DNS Operations, Analysis, and Research Center)
Charlotte, USA

2 au 7 mars 2024
ICANN 79 : Forum de la communauté
San Juan, Porto Rico

16 au 22 mars 2024
IETF 119
Brisbane, Australie

20 au 24 mai 2024
RIPE 88
Varsovie, Pologne

27 au 31 mai 2024
UIT Forum du SMSI 20
Genève, Suisse

10 au 13 juin 2024
ICANN 80 : Forum des politiques
Kigali, Rwanda

afnic
Internet made in France

VOTRE CONTACT

lalettre@afnic.fr

Directeur de publication : Pierre Bonis

Afnic | www.afnic.fr
Immeuble Stephenson,
1 rue Stephenson,
78180 Montigny-le-Bretonneux