afnic
Internet
made in France

La lettre n°12

1

La transition vers la cryptographie post-quantique doit s'engager sans attendre

Nous l'évoquions déjà dans La Lettre Afnic n°10[1], la menace que représentent les ordinateurs quantiques pour la cryptographie actuelle a dépassé le stade de la simple théorie. À tel point qu'elle est désormais intégrée aux stratégies des autorités nationales et internationales de cybersécurité qui convergent toutes vers une même conclusion : la transition vers des mécanismes cryptographiques résistants au calcul quantique doit être engagée dès maintenant. Pour un opérateur d'infrastructures essentielles tel que l'Afnic, cette transition s'inscrit aujourd'hui dans une réalité opérationnelle, avec des implications concrètes pour le DNS et ses extensions de sécurité, notamment DNSSEC.

En France, la stratégie de l'ANSSI fixe le cap de la transition

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a clairement positionné la cryptographie postquantique (PQC) comme un enjeu stratégique de long terme. L'agence appelle ainsi les organisations à engager sans attendre une démarche structurée de préparation, fondée sur trois étapes clés : l'inventaire des usages cryptographiques, l'identification des systèmes critiques et l'élaboration d'un plan de transition.

Cette approche tient compte de la réalité de systèmes d'information complexes, où la cryptographie est souvent omniprésente, parfois implicite et profondément imbriquée dans des composants hétérogènes, y compris des systèmes anciens ou périphériques. La transition ne peut donc pas se résumer à un simple changement d'algorithme, mais s'apparente plutôt à une transformation progressive et profonde des architectures de sécurité.

Concrètement, plusieurs jalons ont été annoncés[2] par l'ANSSI. À partir de 2027, l'intégration de mécanismes postquantiques deviendra un prérequis pour l'entrée en qualification des produits de sécurité auprès de l'ANSSI. Et à l'horizon 2030, l'agence considère qu'il ne sera plus raisonnable d'acquérir des solutions ne prenant pas en compte la cryptographie postquantique.

Ces échéances, rappelées par Samih Souissi, chef d'état-major de la sous-direction Expertise de l'ANSSI, lors de la Journée du Conseil Scientifique de l'Afnic (JCSA) le 14 novembre 2025, visent à inciter les responsables techniques à se mobiliser dès aujourd'hui pour éviter un effet de rupture à l'horizon 2030, lorsque l'achat de solutions non compatibles PQC deviendra progressivement inacceptable dans les marchés de la sécurité.

L'ANSSI souligne également l'importance d'éviter toute régression de sécurité dans la transition vers la cryptographie post-quantique. Bien que conçus pour résister aux attaques quantiques futures, les algorithmes post-quantiques sont plus récents et disposent d'un recul opérationnel encore limité par rapport aux mécanismes éprouvés de cryptographie traditionnelle. Ils restent donc exposés à des attaques dites « classiques », indépendantes de l'existence d'ordinateurs quantiques. Dans ce contexte, l'ANSSI recommande le recours à des approches hybrides, combinant un algorithme classique et un algorithme post-quantique au sein d'un même mécanisme, afin de garantir une continuité de sécurité tout au long de la phase de transition et de permettre une adoption progressive, sans jamais affaiblir la protection des systèmes existants.

1. *« Cryptographie post-quantique : préparer l'infrastructure internet à une transition technique inévitable »* dans La Lettre Afnic n°10
2. https://www.cyber.gouv.fr/enjeux-technologiques/cryptographie-post-quantique/

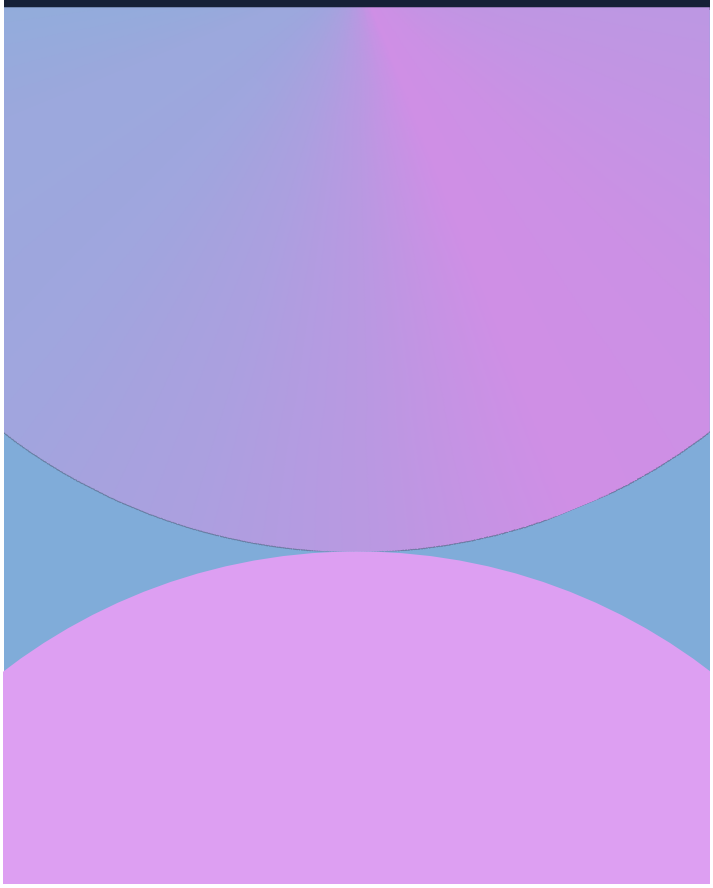
Où en est vraiment l'ordinateur quantique ?

Les ordinateurs quantiques font l'objet d'investissements massifs et de progrès réguliers, mais ils restent aujourd'hui très éloignés des capacités nécessaires pour remettre en cause la cryptographie utilisée à grande échelle sur internet.

Contrairement aux ordinateurs classiques, leur puissance ne se mesure pas seulement au nombre de qubits (ou bits quantiques) annoncés, mais aussi à leur qualité : stabilité, taux d'erreur et capacité à corriger ces erreurs. Or, si les machines actuelles peuvent afficher un nombre croissant de qubits, leur fiabilité reste encore limitée.

En pratique, elles ne disposent donc pas encore d'une puissance de calcul quantique exploitable de manière fiable et soutenue pour exécuter des attaques cryptographiques à grande échelle. Et au-delà de cette puissance de calcul, l'état actuel des technologies suppose également des conditions de fonctionnement extrêmement contraignantes, notamment des températures proches du zéro absolu et des infrastructures lourdes.

Les ordinateurs quantiques dits « cryptographiquement pertinents », capables de casser des mécanismes comme RSA ou les courbes elliptiques largement utilisés aujourd'hui sur internet pour chiffrer les communications et signer des données, n'existent donc pas à ce stade. Les estimations situent cet horizon à dix à quinze ans.



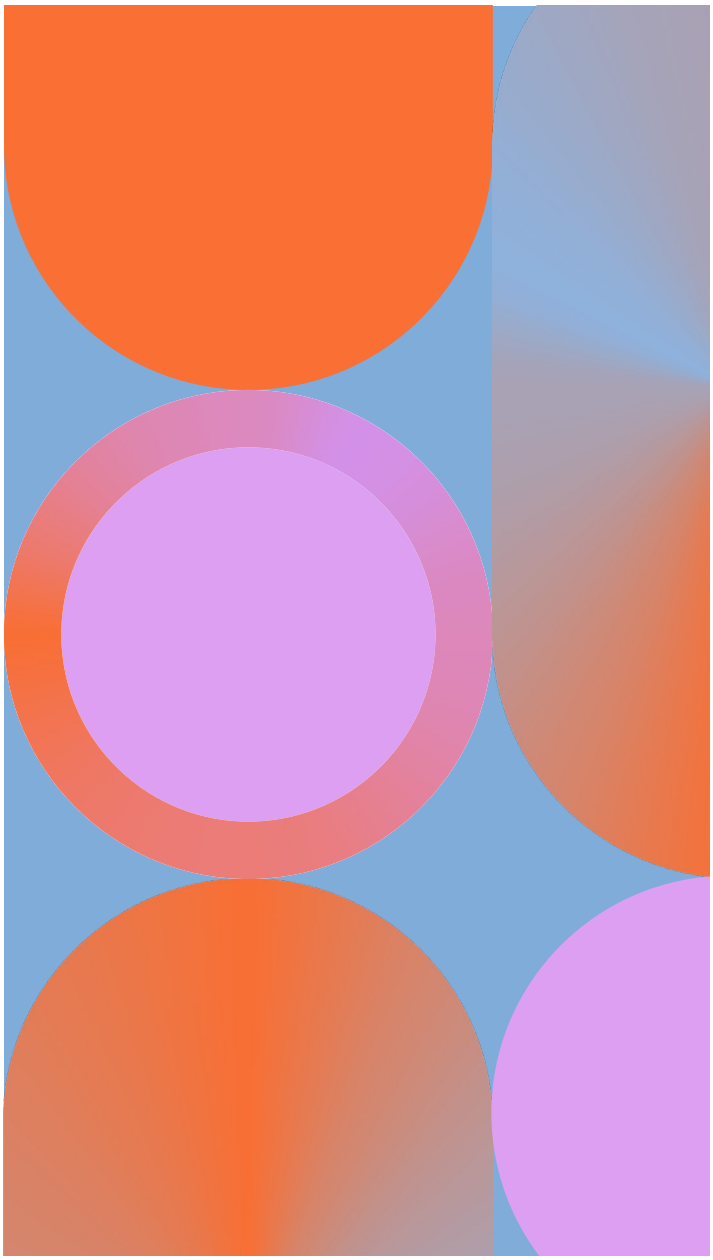
À l'international, le NIST appelle aussi à engager la transition dès maintenant

Le NIST (*National Institute of Standards and Technology*) joue un rôle central dans la structuration de la transition vers la cryptographie postquantique en pilotant des travaux de standardisation d'algorithmes pertinents qui servent aujourd'hui de référence au niveau international. Dans son rapport NIST IR 8547[3], publié sous forme de projet fin 2024, l'institut recommande explicitement de planifier la transition sans attendre.

Le document s'appuie notamment sur le théorème de Mosca, qui met en évidence le risque dit de « *store now, decrypt later* ». Ce principe d'attaque par anticipation repose sur une idée simple : même en l'absence d'ordinateurs quantiques capables de casser des algorithmes cryptographiques, des attaquants peuvent dès aujourd'hui collecter des données chiffrées et les stocker dans l'attente que des capacités futures permettent de les déchiffrer et de les lire. Parce que certaines informations confidentielles ont une longue durée de vie et de valeur, la préparation doit être engagée dès à présent.

À l'instar de l'ANSSI, le NIST reconnaît cependant la complexité de la transition, en particulier pour les usages impliquant des modules matériels de sécurité (HSM) ou des mécanismes de signature à grande échelle. Il recommande une approche pragmatique, combinant inventaire, priorisation des actifs sensibles et intégration progressive de solutions postquantiques, idéalement sous forme hybride en combinaison avec des algorithmes classiques.

Cette position est largement partagée par d'autres acteurs institutionnels et industriels, et converge avec les orientations européennes en matière de cybersécurité. Le message est clair : la transition vers la PQC est un processus de long terme qui doit être amorcé dès aujourd'hui.



3. https://csrc.nist.gov/pubs/ir/8547/ipd

De premiers algorithmes post-quantiques identifiés

La transition vers la cryptographie post-quantique ne repose plus uniquement sur des travaux prospectifs : des algorithmes de référence ont été identifiés dans le cadre des travaux de standardisation menés par le NIST depuis 2016.

En 2022, une première vague d'algorithmes ont ainsi été sélectionnés, couvrant les usages essentiels : CRYSTALS-Kyber pour l'échange de clés, ainsi que CRYSTALS-Dilithium, Falcon et SPHINCS+ pour les signatures numériques. Plus récemment en 2025, le NIST a également retenu HQC (Hamming Quasi-Cyclic) comme algorithme supplémentaire pour l'échange de clés.

Ces algorithmes sont aujourd'hui utilisés dans des tests et des expérimentations, principalement dans des environnements logiciels. Leur intégration opérationnelle à grande échelle, notamment dans des infrastructures critiques ou fortement contraintes, comme les modules matériels de sécurité (HSM) ou des services tels que le DNS, reste à construire et dépend encore des processus d'évaluation et de standardisation en cours.

Que faut-il retenir des tests menés par l'Afnic sur le DNS ?

Pour un registre comme l'Afnic, la question des algorithmes post-quantiques touche directement des éléments du cœur de l'internet, notamment les mécanismes de signature cryptographique asymétrique permettant d'authentifier les enregistrements DNS. C'est dans cette perspective que l'Afnic a mené des tests sur l'ensemble de la zone .fr, portant sur l'utilisation d'algorithmes post-quantiques dans DNSSEC et couvrant à la fois la signature des zones, la vérification des signatures et les impacts associés sur le volume de données et les performances.

Les résultats de ces premiers tests, présentés lors de la JCSA 2025, mettent en évidence un effet cumulatif des algorithmes post-quantiques sur l'ensemble de la chaîne DNSSEC. La taille des clés et des signatures augmente ainsi fortement par rapport aux algorithmes classiques, ce qui se traduit directement par un fichier de zone significativement plus gros et des volumes de données manipulés et échangés bien plus importants. Cela a des conséquences opérationnelles immédiates : les temps de signature sont cinq à dix fois plus lents et les ressources de calcul, de stockage et de réseau sont davantage sollicitées. À l'échelle d'une zone comme celle du .fr, ces effets combinés montrent que le passage au post-quantique ne peut pas être abordé comme un simple changement d'algorithme.

Au-delà de ces premiers résultats expérimentaux et des réflexions qu'ils soulèvent, l'Afnic identifie plusieurs chantiers structurants liés à l'intégration effective et efficace de la cryptographie post-quantique dans le DNS :

- **La stabilisation des standards, en particulier pour les usages DNSSEC.** Les mécanismes permettant d'intégrer des algorithmes post-quantiques dans DNSSEC ne font pas encore l'objet de standards finalisés. Leurs expérimentations et leur évolution conditionneront la possibilité de déploiements interopérables et pérennes à l'échelle de l'internet.
- **L'éventuelle évolution des mécanismes de validation DNSSEC pour les serveurs récursifs (ou résolveurs).** Les logiciels actuels observés privilégient la sélection automatique de l'algorithme associé à l'identifiant le plus bas et non le plus adapté, une méthode qui fonctionnait jusqu'à maintenant mais qui pourrait s'avérer sous-optimale face aux contraintes spécifiques des algorithmes post-quantiques.
- **La mise en place de signatures hybrides.** La combinaison d'algorithmes classiques et post-quantiques au sein d'un même mécanisme apparaît comme une piste pertinente pour éviter toute régression de sécurité, mais elle soulève des questions d'interopérabilité et de cohérence de mise en œuvre entre les acteurs.
- **L'analyse de l'impact sur les serveurs faisant autorité.** L'augmentation des volumes de données et des temps de calcul observée lors des tests impose d'évaluer finement les conséquences sur les performances, la résilience et l'exploitation des infrastructures de serveurs faisant autorité.
- **Le suivi du déploiement et de la compatibilité des résolveurs dits « validants », publics comme privés.** La capacité des résolveurs à prendre en charge de nouveaux mécanismes cryptographiques conditionnera leur adoption effective, ainsi que la continuité de service pour les utilisateurs finaux.
- **L'évaluation des solutions de type HSM.** La disponibilité et les performances dans les modules matériels de sécurité restent encore à confirmer. Ces composants étant importants pour la signature à grande échelle, des tests préliminaires sont d'ores et déjà engagés afin d'en apprécier les contraintes et les possibilités d'évolution.

Ces axes de travail confirment que la transition vers la cryptographie post-quantique appliquée au DNS est un chantier complexe, qui devra être conduit de manière progressive et coordonnée avec l'ensemble de l'écosystème.

La cryptographie post-quantique n'impose pas une rupture brutale, mais un changement de posture. Elle oblige à penser la sécurité dans la durée.

Anticiper sans précipiter

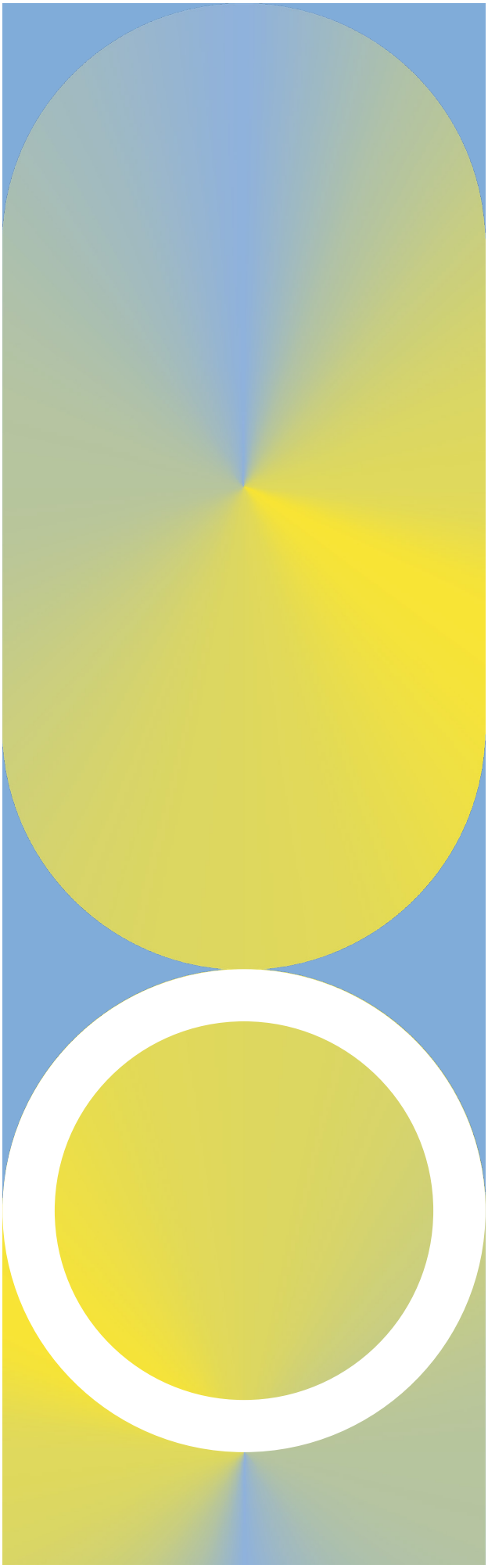
La cryptographie post-quantique n'impose pas une rupture brutale, mais un changement de posture. Elle oblige à penser la sécurité dans la durée, à accepter des compromis temporaires et à travailler avec des standards encore en mouvement. Pour les infrastructures essentielles comme le DNS, cela signifie sortir d'une logique purement algorithmique pour aborder des questions d'architecture, d'interopérabilité et de soutenabilité opérationnelle.

Les années à venir ne seront probablement pas celles d'un basculement généralisé, mais d'expérimentations, d'ajustements et de choix structurants faits collectivement. Dans ce contexte, tester tôt, partager les retours d'expérience et contribuer aux travaux de standardisation n'est pas un luxe. C'est une condition pour que la transition se fasse sans fragiliser la sécurité et la confiance dans l'internet.

02

Revue à 20 ans du SMSI : le texte final a été adopté par consensus à New York

C'est l'aboutissement d'un processus attendu de longue date : vingt ans après les sommets de Genève en 2003 et de Tunis en 2005, qui avaient posé les bases du cadre international de la gouvernance de l'internet, le SMSI+20 ne visait pas seulement à dresser un bilan des vingt années écoulées, mais aussi à vérifier si les principes issus du Sommet mondial sur la société de l'information (SMSI) restaient pertinents dans un contexte profondément transformé, où les enjeux numériques sont devenus éminemment politiques[4].



Tout au long de l'année 2025, les négociations ont mobilisé les États membres et les autres parties prenantes de l'internet, au fil de consultations et de versions successives du texte. Ce travail progressif, marqué par la recherche de points d'équilibre entre des positions souvent divergentes, s'est intensifié dans les dernières semaines de l'année. Le texte a finalement été adopté par consensus le 17 décembre 2025 lors d'une séance plénière de l'Assemblée générale des Nations Unies à New York[5], signe que tous l'ont jugé suffisamment satisfaisant pour ne pas nécessiter de vote. Sur un sujet tel que la gouvernance de l'internet, parvenir ainsi à un tel accord n'a rien d'une évidence dans le contexte actuel.

Des inquiétudes clairement identifiées dès le départ

La revue à 20 ans du SMSI s'était en effet ouverte début 2025 dans un contexte de débats nourris sur l'avenir de la gouvernance de l'internet et plus largement du numérique. Si le principe d'une revue faisait consensus, les discussions ont rapidement montré que tous les acteurs n'avaient pas la même lecture de ce que devait devenir le cadre issu du SMSI et de l'évolution souhaitable de la gouvernance de l'internet. Dans ce contexte, certains acteurs, en particulier au sein de la communauté technique, ont exprimé des préoccupations quant à la préservation des principes et mécanismes construits depuis vingt ans.

Ces craintes ont notamment porté sur une possible remise en cause du modèle multi-parties prenantes de la gouvernance de l'internet. Depuis plusieurs années, celui-ci est en effet régulièrement contesté par certains États, qui plaident pour une approche davantage centrée sur des mécanismes gouvernementaux et multilatéraux. Le SMSI+20 représentait donc une étape importante : soit le texte réaffirmait clairement le principe fondateur d'une gouvernance multipartite, soit il se dirigeait vers un modèle plus strictement interétatique.

Le Forum sur la gouvernance de l'internet (FGI) était également sur la sellette. Son mandat arrivait en effet à échéance et plusieurs options étaient sur la table : sa reconduction, sa marginalisation progressive ou son remplacement par d'autres mécanismes plus intergouvernementaux. La question n'était pas technique, mais politique. Le FGI reste en effet l'un des rares espaces où États, secteur privé, société civile, communauté technique et monde académique dialoguent sur un pied relativement égal.

4. Cette question a été analysée en détail dans l'article *« SMSI+20 : la gouvernance d'internet à l'heure du grand bilan »* de La Lettre Afnic n°9
5. Le texte adopté est accessible via la page officielle du processus SMSI+20 du Département des affaires économiques et sociales (DAES) des Nations Unies, qui rassemble également les principales informations et ressources relatives à son déroulement : https://publicadministration.desa.un.org/fr/node/2824

Un texte globalement satisfaisant

Le document adopté en décembre 2025 ne lève pas toutes les ambiguïtés, mais il sécurise l'essentiel.

Le modèle multi-parties prenantes est clairement réaffirmé. Le document rappelle que la gouvernance de l'internet repose sur la complémentarité des rôles des États, du secteur privé, de la société civile, des organisations internationales, de la communauté technique et du monde académique.

Cette position s'inscrit dans la continuité des principes du SMSI défendus lors de NETmundial+10 en avril 2024[6] et adoptés dans les engagements du Pacte Numérique Mondial en septembre de la même année[7], en faveur d'une gouvernance de l'internet fondée sur la participation de l'ensemble des parties prenantes. En la réaffirmant à son tour, le SMSI+20 confirme ainsi, vingt ans après Genève et Tunis, le maintien d'une logique de stabilité plutôt que de rupture.

Le FGI est permanentisé. Le texte confirme en effet le caractère permanent du FGI au sein des Nations Unies. Il encourage également une meilleure articulation avec les autres mécanismes onusiens, afin de renforcer son utilité et son caractère opérationnel. Le scénario d'un affaiblissement ou d'une mise à l'écart du FGI est donc écarté. Le texte mentionne également explicitement les FGI nationaux et régionaux, dont le FGI France, reconnaissant ainsi que la gouvernance de l'internet ne se construit pas uniquement à l'échelle globale, mais aussi au plus près des territoires.

Cette décision s'accompagne toutefois d'une limite importante : la question du financement. Contrairement à d'autres mécanismes onusiens, aucun cadre de financement pérenne et garanti n'est acté à ce stade. Le texte renvoie à des discussions ultérieures, ce qui laisse subsister une incertitude sur la capacité du FGI à maintenir son niveau d'activité et de pertinence dans la durée. Cette fragilité est d'autant plus notable que l'écosystème international du numérique continue de se densifier, avec le risque de voir émerger des initiatives concurrentes, mieux dotées ou plus visibles.

Le multilinguisme trouve une place explicite dans le texte. Le paragraphe qui lui est consacré dépasse la seule question culturelle. Il aborde l'accès aux services en ligne, la sécurité et la robustesse de l'internet, notamment à travers la reconnaissance des noms de domaine internationalisés et de l'acceptation universelle. Pour les acteurs engagés de longue date sur ces sujets, dont l'Afnic fait partie, cette mention marque une reconnaissance bienvenue d'un enjeu encore trop souvent perçu comme secondaire[8].

Le SMSI+20 reconnaît également la nécessité de faire évoluer les lignes d'action historiques du SMSI. Définies au début des années 2000, alors que les débats portaient principalement sur la connectivité et la fracture numérique, ces lignes d'action sont aujourd'hui confrontées à un élargissement marqué des enjeux, allant de la cybersécurité à l'intelligence artificielle et à la régulation des plateformes. Le texte adopté n'entre toutefois pas dans une révision détaillée de ces lignes. Il appelle plutôt à inscrire leur mise en œuvre dans des feuilles de route plus opérationnelles, alignées avec l'Agenda 2030 et le Pacte Numérique Mondial, sans pour autant préciser de calendrier ni de modalités précises.

Le SMSI+20 se conclut donc sur un texte d'équilibre. Il confirme les principes fondamentaux issus de 2005, tout en les replaçant dans leur environnement actuel.

Un point d'aboutissement, pas un point final

Le SMSI+20 se conclut donc sur un texte d'équilibre. Il confirme les principes fondamentaux issus de 2005, tout en les replaçant dans leur environnement actuel, profondément transformé, marqué à la fois par des évolutions technologiques majeures et de nouveaux enjeux pleinement politiques, économiques et géopolitiques.

La suite se jouera désormais sur des questions de mise en œuvre très concrètes : les moyens alloués au FGI, sa capacité à rester un espace central face à la multiplication des initiatives internationales et la participation effective des parties prenantes à la mise en œuvre des engagements pris. Le texte prévoit par ailleurs un nouveau rendez-vous à l'horizon 2035, confirmant que le SMSI et la gouvernance de l'internet s'inscrivent dans un processus de suivi et d'adaptation sur le long terme.

6. Voir à ce sujet l'article « *NETmundial+10 : réaffirmer les principes d'une gouvernance d'internet multi-acteurs* » de La Lettre Afnic n°6, qui revient sur l'adoption, lors de NETmundial+10, d'une déclaration réaffirmant les principes fondateurs de la gouvernance de l'internet et le rôle central du modèle multi-parties prenantes.
7. Dans l'article « *Le Pacte Numérique Mondial a été adopté* » de La Lettre Afnic n°7, nous en analysions les principaux engagements, notamment la reconnaissance, dans un cadre onusien, d'une gouvernance de l'internet fondée sur la participation de l'ensemble des parties prenantes.
8. Pour mieux comprendre en quoi le multilinguisme est un enjeu clé pour un internet véritablement mondial, consulter l'article « *Universal Acceptance : les défis d'un internet linguistiquement inclusif* » de La Lettre Afnic n°4.

03

Extensions internet personnalisées : l'*Applicant Guidebook* de l'ICANN précise le cadre et le déroulé du processus de candidature

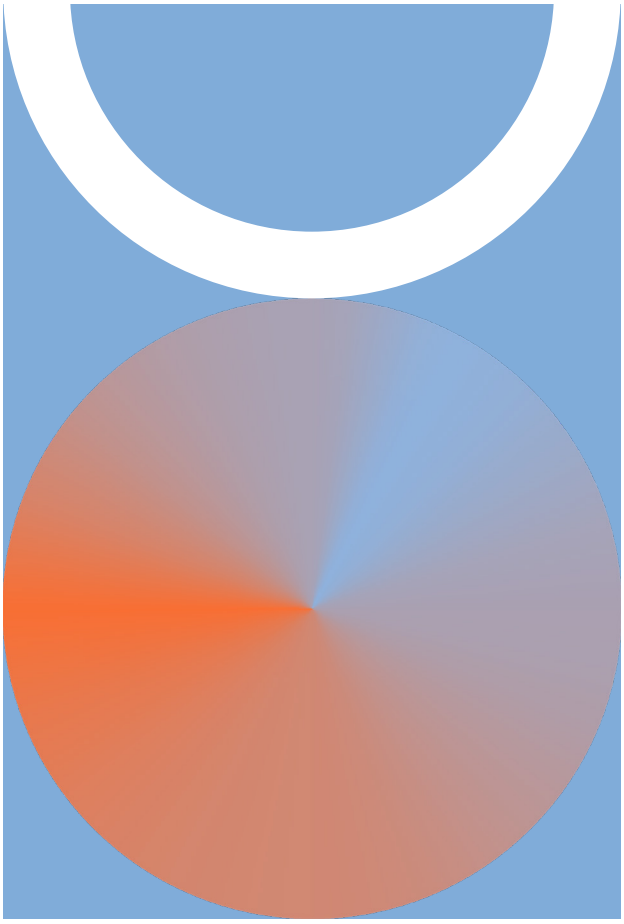
La prochaine fenêtre de candidature pour l'obtention d'une extension personnalisée auprès de l'ICANN, l'organisation chargée de coordonner et de superviser les aspects techniques et opérationnels des systèmes des noms de domaine et des adresses IP sur internet, ouvrira le 30 avril prochain. Les entreprises, collectivités, organisations communautaires ou consortiums intéressés auront alors jusqu'au 12 août 2026 pour soumettre leur dossier. Avec la publication, en décembre dernier, de la version finale de son *Applicant Guidebook*[9] (guide du candidat), l'ICANN a apporté plus de précisions sur le cadre de la procédure et de visibilité sur les prochaines grandes étapes du parcours candidat.

Un cadre plus structuré et une procédure plus fluide qu'en 2012

Tirant les enseignements du précédent cycle de candidatures de 2012[10], l'ICANN a fait évoluer son cadre de référence : le nouvel *Applicant Guidebook* intègre ainsi plusieurs modifications apportées aux directives de dépôt et au suivi d'une candidature, visant notamment à rendre la procédure plus fluide et plus lisible.

On note tout particulièrement :

- **La reconnaissance explicite des extensions .brand (ou .marque).** Désormais identifiées comme une catégorie à part entière, elles font l'objet de règles et d'exigences spécifiques, mieux adaptées aux usages généralement fermés des extensions de marque.
- **La possibilité d'ajouter jusqu'à quatre variantes de l'extension demandée dans une même candidature**, afin de mieux gérer les situations de similarité entre chaînes de caractères proches ou susceptibles d'être confondues et de limiter les risques de blocage lors de l'évaluation, notamment en cas d'opposition ou de contentieux.
- **Davantage de lisibilité sur le déroulement de la procédure.** Les principales phases, leur durée et leur enchaînement sont précisés. Sans lever l'ensemble des incertitudes inhérentes à un processus de cette ampleur, cela permet aux organisations intéressées de mieux se projeter dans le calendrier et d'anticiper les étapes clés.



Un coût de base clairement établi, un budget final dépendant des évaluations conditionnelles

L'ICANN avait déjà communiqué, dès septembre 2024[11], sur un coût d'entrée fixé à 227 000 USD par candidature. La version finale de l'*Applicant Guidebook* vient confirmer ce montant et préciser les cas où des évaluations conditionnelles peuvent s'ajouter, engendrant des frais supplémentaires.

Le principe même d'évaluations complémentaires assorties de frais additionnels ne constitue pas en soi une préoccupation. Ces frais ont vocation à couvrir les coûts effectivement supportés par l'ICANN, notamment lorsque l'examen d'une candidature nécessite l'intervention de panels d'experts spécifiques. En revanche, l'*Applicant Guidebook* ne précise pas toujours de manière suffisamment détaillée ce que vont couvrir ces évaluations, sur quels critères elles seront déclenchées, ni même quel sera leur coût précis.

Ainsi, par exemple, les candidatures pour des extensions géographiques pourront engendrer des frais additionnels « jusqu'à 12 000 USD », tandis que celles portant sur des extensions communautaires pourront entraîner des coûts d'évaluation conditionnelle compris « entre 50 000 et 80 000 USD ». Pour les candidats, ces fourchettes de montants sont suffisamment larges pour complexifier leur anticipation du coût définitif de leur projet.

Un calendrier plus lisible sur l'ensemble du cycle

L'*Applicant Guidebook* apporte également des éléments plus concrets sur le calendrier du processus global. Il décrit les principales étapes qui jalonnent le parcours d'une candidature, leur durée et leur enchaînement. Une fois la fenêtre de dépôt (du 30 avril au 12 août 2026) refermée, les candidatures entreront ainsi dans les phases successives prévues par l'ICANN : vérifications administratives, évaluations techniques et financières, traitement des éventuelles oppositions ou situations de contentieux, puis contractualisation et, enfin, délégation.

La durée exacte de l'ensemble du processus dépendra de plusieurs critères, notamment des caractéristiques propres à chaque candidature, des évaluations requises, mais aussi du nombre total de candidatures reçues par l'ICANN. À ce stade, l'*Applicant Guidebook* estime que le cycle complet pourra s'étendre sur une période comprise entre 14,5 et 19,5 mois. Cette projection, formulée de manière plus explicite qu'en 2012, offre aux candidats une meilleure visibilité sur l'enchaînement des étapes et les délais attendus.

9. https://newgtldprogram.icann.org/en/application-rounds/round2/agb
10. Lire l'article « *Nouvelles extension de domaine : le prochain round à l'ICANN est prévu en 2026* » dans La Lettre Afnic n°5 pour une analyse du précédent cycle de candidatures de 2012 et des enseignements tirés.
11. https://www.icann.org/fr/blogs/details/icann-sets-expected-evaluation-fee-for-new-gtld-applications-in-the-next-round-25-09-2024-fr

04

Brèves

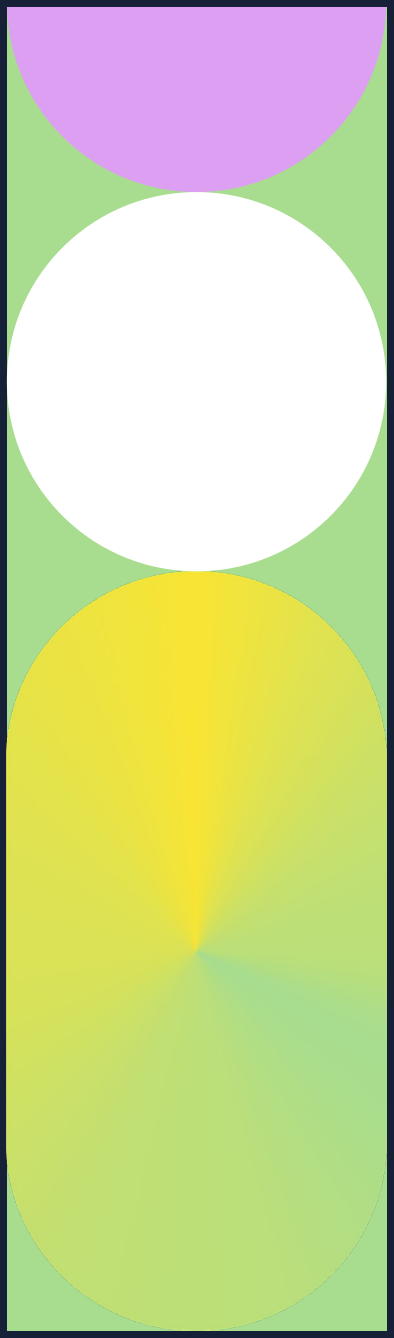
Les initiatives autour des communs numériques se multiplient

La notion de « communs numériques » gagne progressivement en visibilité dans les réflexions sur l'évolution d'internet et de ses infrastructures. Plusieurs initiatives récentes traduisent en effet une volonté de promouvoir ces ressources numériques d'intérêt général, telles que des infrastructures, des logiciels ou des standards ouverts, conçues pour être partagées et gouvernées collectivement.

Le Consortium pour une infrastructure numérique européenne pour les communs numériques[12] (DC-EDIC ou *Digital Commons European Digital Infrastructure Consortium* en anglais) a ainsi été annoncé lors du Sommet sur la souveraineté numérique européenne, organisé conjointement par la France et l'Allemagne à Berlin en novembre 2025. À l'initiative de la France, de l'Allemagne, des Pays-Bas et de l'Italie, il vise à structurer une communauté européenne des communs numériques, notamment en facilitant l'accès au financement et en soutenant le développement de projets reposant sur des ressources numériques ouvertes et partagées. Cette initiative s'inscrit dans le cadre juridique du Consortium pour une infrastructure numérique européenne[13] (EDIC ou *European Digital Infrastructure Consortium* en anglais), un instrument juridique qui permet à plusieurs États membres de se regrouper au sein d'une entité commune afin de faciliter la conception, le déploiement et l'exploitation de projets numériques plurinationaux, au service de priorités identifiées au niveau de l'Union. Les quatre États fondateurs ont déjà été rejoints par le Luxembourg, la Slovénie et la Pologne qui participent en tant qu'observateurs.

L'initiative Current AI[14], quant à elle, a été lancée lors du Sommet pour l'action sur l'Intelligence Artificielle qui s'est déroulé à Paris en février 2025. Constituée sous la forme d'une association de loi 1901 enregistrée en France, Current AI repose sur un partenariat public-privé regroupant, à l'échelle mondiale, des gouvernements, des organisations philanthropiques, des entreprises technologiques et des acteurs de la recherche. Le projet vise à faire émerger une intelligence artificielle d'intérêt général, c'est-à-dire ouverte, transparente et inclusive. Avec un financement initial annoncé d'environ 400 millions de dollars engagés par une coalition d'acteurs publics, philanthropiques et privés, l'initiative a pour objectif de lever jusqu'à 2,5 milliards de dollars d'ici 2030 pour soutenir des projets d'IA d'intérêt général.

Ces différentes initiatives traduisent la recherche de nouveaux équilibres entre innovation, intérêt général et gouvernance des infrastructures numériques, dans un contexte marqué par la concentration des acteurs et des usages. Elles s'inscrivent également dans le prolongement des réflexions sur les infrastructures publiques numériques (IPN), entendues comme des infrastructures essentielles conçues comme des biens publics et gouvernées de manière collective, et interrogent plus largement la capacité des acteurs publics et des communautés techniques à structurer, dans la durée, des modèles alternatifs capables de soutenir un internet ouvert, interopérable et résilient.



12. https://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1761826156429&uri=CELEX%3A32025D2170
13. https://digital-strategy.ec.europa.eu/fr/policies/edic
14. https://www.currentai.org/fr

NIS2 : un forum multi-acteurs pour ancrer les standards internet dans la réalité opérationnelle

Les 21 et 22 janvier derniers, la Commission européenne a organisé à Bruxelles la première réunion du *Multi-Stakeholder Forum on Internet Standards Deployment* (Forum multi-acteurs sur le déploiement des standards internet)[15], avec près d'une centaine de participants issus des secteurs public et privé, ainsi que de la communauté technique.

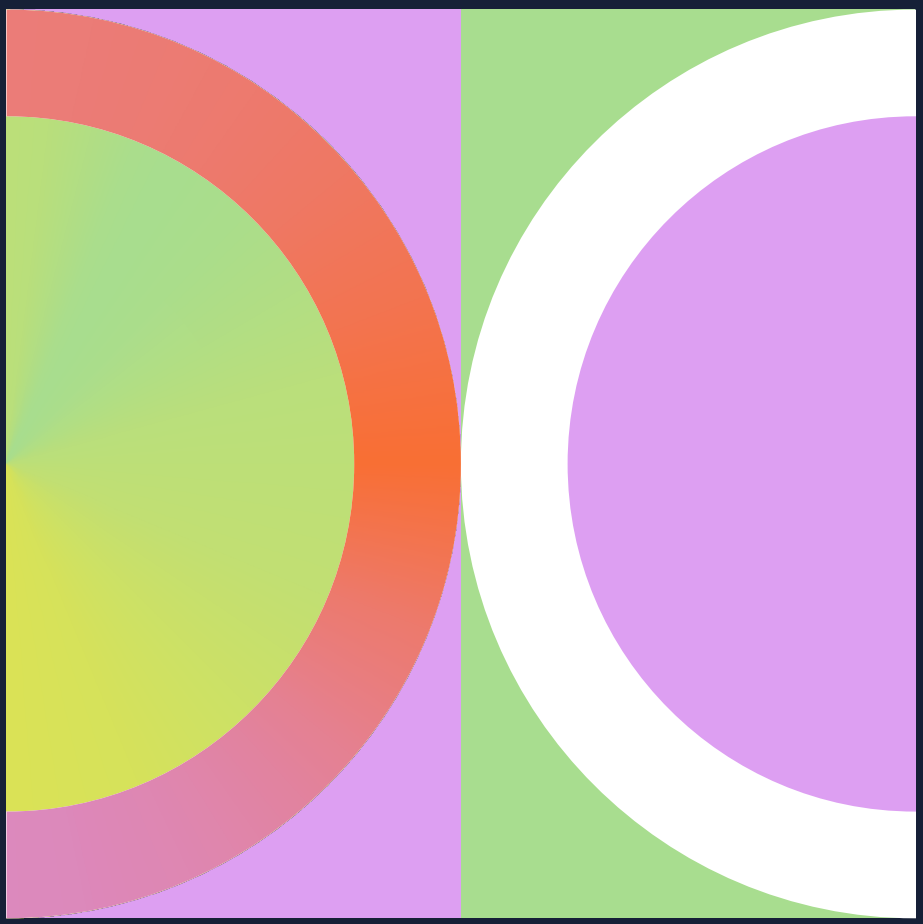
Le Forum multi-acteurs sur le déploiement des standards internet s'inscrit directement dans le cadre de la mise en œuvre de la directive NIS2 qui renforce les exigences européennes en matière de cybersécurité[16]. Son objectif est clair : identifier les standards et les bonnes pratiques réellement déployables afin d'accompagner les entreprises et organisations concernées par NIS2 dans une mise en conformité pragmatique et opérationnelle. Il ne s'agit pas ici de créer de nouveaux protocoles, mais bien de capitaliser sur l'existant, de confronter les standards aux pratiques de terrain et d'éclairer les futures politiques européennes en la matière.

La session d'ouverture a été assurée par Vint Cerf, souvent considéré comme l'un des « pères de l'internet », aujourd'hui *Chief Internet Evangelist* chez Google. Il a rappelé deux principes clés pour l'évolution des standards internet : l'importance de la rétrocompatibilité, c'est-à-dire la capacité d'une nouveauté technique à fonctionner avec les environnements existants, et la nécessité pour les protocoles d'être réellement déployables et pas seulement théoriquement solides. Ces principes ont servi de fil conducteur à l'ensemble des discussions qui ont suivi.

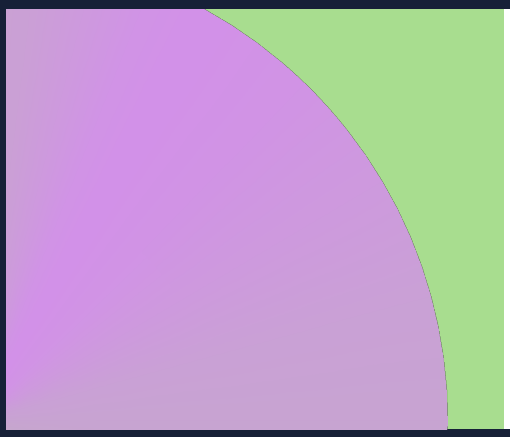
Le Forum a ensuite été structuré autour de quatre « *workstreams* » correspondant à des priorités identifiées dans les textes d'application de NIS2 : les protocoles de communication de la couche réseau, la sécurité du courrier électronique, la sécurité du DNS et la sécurité et l'hygiène du routage internet. Chacun de ces axes, abordés de manière séquentielle lors de l'événement, a donné lieu à des présentations de la Commission européenne suivies de discussions ouvertes entre participants. Les échanges consacrés à la sécurité du DNS, auxquels l'Afnic a activement participé, ont notamment confirmé, de manière très concrète, la nécessité d'intégrer les contraintes techniques, organisationnelles et économiques dans les futures recommandations.

Les travaux du Forum se poursuivront sur une période de deux ans, principalement à distance, avec des réunions tous les deux à trois mois. Les prochaines rencontres sont prévues du 24 au 26 mars 2026, puis fin juin 2026. Les livrables, attendus à l'horizon du 4ème trimestre 2027, comprendront des rapports et recommandations identifiant les standards pertinents et les bonnes pratiques dans chacun des quatre axes retenus. Ces travaux pourront ensuite servir de référence pour les politiques européennes et contribuer à des mécanismes d'incitation visant à encourager le déploiement de bonnes pratiques.

15. https://digital-strategy.ec.europa.eu/en/news/european-commission-seeks-participants-multi-stakeholder-forum-internet-standards-deployment-0
16. Pour un éclairage général sur les objectifs et les enjeux de NIS2, consulter l'article « *La directive NIS2 va indéniablement renforcer la cybersécurité au sein de l'Union européen, mais attention aux effets de bord* » paru dans La Lettre Afnic n°6

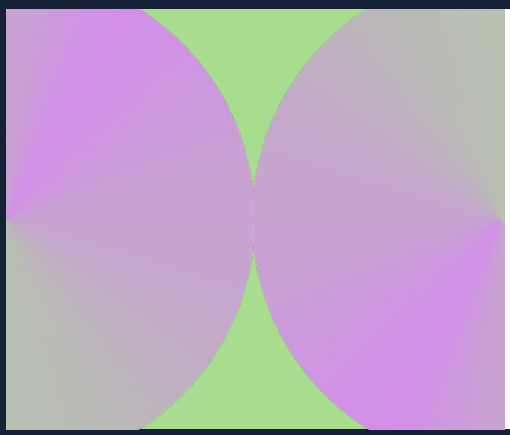


5 L'Afnic y était



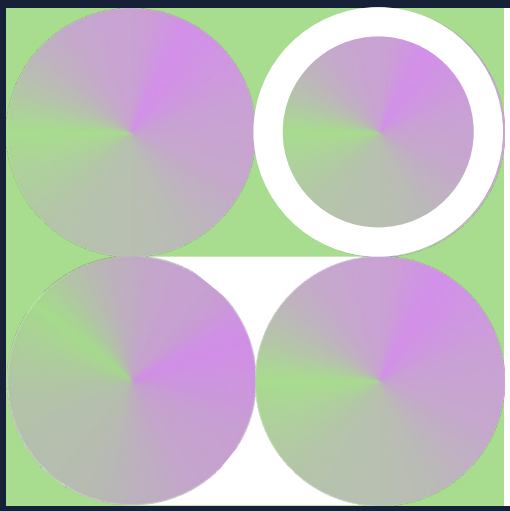
Comité Technique de LoRa Alliance, les 3 et 4 février 2026, Guyancourt, France

L'Afnic et Kerlink accueillaient en février dernier le 35ème Comité Technique de LoRa Alliance, dédié aux développements des standards LoRaWAN, technologie de communication sans fil conçue pour l'Internet des objets (IoT) et permettant de transmettre de petites quantités de données sur de longues distances tout en consommant très peu d'énergie. L'Afnic, qui préside le groupe de travail académique, y contribue activement pour faciliter l'utilisation du DNS dans les fonctionnalités clés de LoRaWAN.



IETF 124, du 1er au 7 novembre 2025, Montréal, Canada

L'Afnic participe aux travaux visant à améliorer l'efficacité énergétique des protocoles internet. Deux groupes y contribuent de manière complémentaire : d'une part, côté IETF, le groupe GREEN (pour *Getting Ready for Energy-Efficient Networking*) dont les travaux portent sur la terminologie employée et de premiers cas d'usage ; et d'autre part, le groupe de recherche IRTF SUSTAIN (pour *Sustainability and the Internet*) qui opère une réflexion sur la consommation des équipements réseaux ou encore sur le cycle de vie des TIC.



Conférences mondiales de développement des télécommunications (CMDT), du 17 au 28 novembre 2025, Bakou, Azerbaïdjan

L'Afnic a contribué au sein de la délégation française à la CMDT sur les questions touchant à internet et au SMSI. Ainsi, sur la résolution 82 portant sur le multilinguisme sur l'internet, plusieurs propositions et positions de la CEPT (Conférence européenne des administrations des postes et télécommunications) ont été intégrées, notamment pour souligner l'importance de l'acceptation universelle des noms de domaine internationalisés (IDN) et de l'internationalisation des adresses électroniques, ainsi que de la collaboration avec les parties prenantes et la communauté technique pour atteindre le multilinguisme sur internet.

Les prochains événements auxquels l'Afnic participe :

- **14 au 20 mars 2026**
  IETF 125
  Shenzhen, Chine

- **24 au 27 mars 2026**
  CEPT
  Prague, République Tchèque

- **28 avril au 8 mai 2026**
  Conseil de l'UIT
  Genève, Suisse

- **16 et 17 mai 2026**
  OARC 46
  Édinbourg, Ecosse

- **18 au 22 mai 2026**
  RIPE 92
  Édinbourg, Ecosse

- **26 et 27 mai 2026**
  EURODIG
  Bruxelles, Belgique

- **8 au 11 juin 2026**
  ICANN 86
  Séville, Espagne

- **18 au 24 juillet 2026**
  IETF 126
  Vienne, Autriche

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