DOSSIER THÉMATIQUE

DNS

pour le service de nommage en IoT

LE POINT DE VUE DE L'AFNIC

afnic

DOSSIER THÉMATIQUE

DE QUOI S'AGIT-IL ?

Le terme « Internet des objets » (*Internet of Things* / IoT) revêt une signification différente selon la communauté/technologie concernée. Le principe de base est de connecter les « objets » du monde physique à l'infrastructure Internet. Il peut s'agir de n'importe quels « objets », allant des ordinateurs aux personnes, en passant par les médicaments et les livres.

Les objets peuvent être connectés à l'infrastructure Internet soit *directement* soit *indirectement*. Un ordinateur ou un téléphone portable peut être connecté directement à l'Internet au moyen d'une pile IP et d'un type de connectivité de couche 2 (Wi-Fi ou Ethernet, par ex.). Les personnes et les livres sont quant à eux connectés à l'Internet de manière indirecte, par le biais de certains équipements intermédiaires ; il s'agit généralement de dispositifs dépourvus d'adresse IP (capteurs, puces RFID ou étiquettes NFC, notamment) apposés sur les objets.

Ces dispositifs supports n'utilisent pas la suite des protocoles Internet (suite TCP/IP) pour communiquer. Ils utilisent en revanche leurs propres technologies de communication, telles que la radiofréquence (RF), le Bluetooth, la NFC (communication en champ proche) ou encore une plateforme sans fil de longue portée et basse consommation (LoRA). Pour relier les appareils non-connectés au réseau IP (Internet), il faut un dispositif « passerelle » capable de gérer la communication à deux niveaux : d'une part, avec les dispositifs non-IP et d'autre part, avec le réseau IP ; ce dispositif passerelle permet ainsi de relier les mondes non-IP et IP.

/// D'OÙ VIENT CE BESOIN DE CONCEVOIR DES OBJETS « INTELLIGENTS » ?

Le concept fondamental de l'IoT est de rendre « intelligents » des objets qui, par défaut, seraient considérés comme « passifs » d'un point de vue technologique.

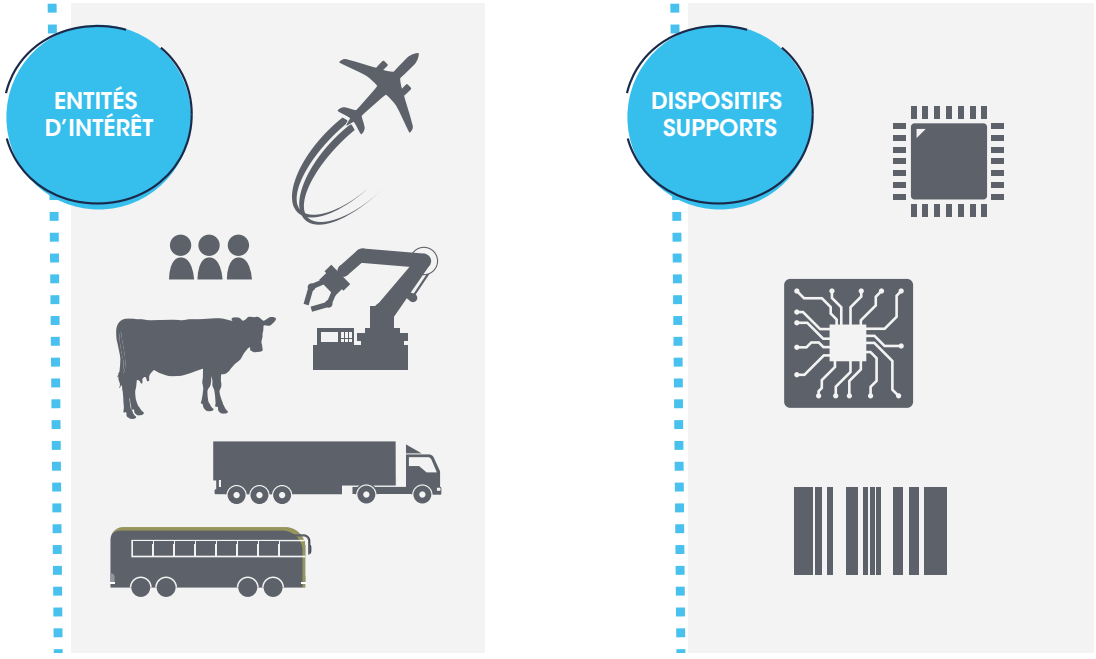


Figure 1 : Rendre les objets intelligents en les marquant avec des dispositifs supports (capteurs, étiquettes RFID, codes à barres, etc.).

Prenons l'exemple d'une vache dans un troupeau. Pour l'éleveur, la vache est une « entité d'intérêt » (Figure 1). Chez la vache, la période optimale de reproduction intervient tous les 21 jours et dure de 12 à 18 heures[1]. Pendant cette période, la vache est plus active que d'ordinaire ; aussi, une application de l'IoT consiste, par exemple, à fixer des podomètres aux pattes de la vache. Ces capteurs envoient périodiquement des informations, et l'éleveur est averti par message lorsque les déplacements de la vache deviennent supérieurs à sa moyenne habituelle. Cet exemple illustre l'étendue des cas d'applications dans lesquels des objets du monde physique reliés à l'infrastructure Internet, deviendraient des objets intelligents.

Les progrès réalisés sur le matériel en termes de rapidité de conception, de miniaturisation, de baisse des coûts et de consommation énergétique ont rendu possible le marquage des objets physiques au moyen de dispositifs IP. C'est la raison pour laquelle le concept d'IoT, quoiqu'il ne soit pas nouveau, fait actuellement couler beaucoup d'encre[2].

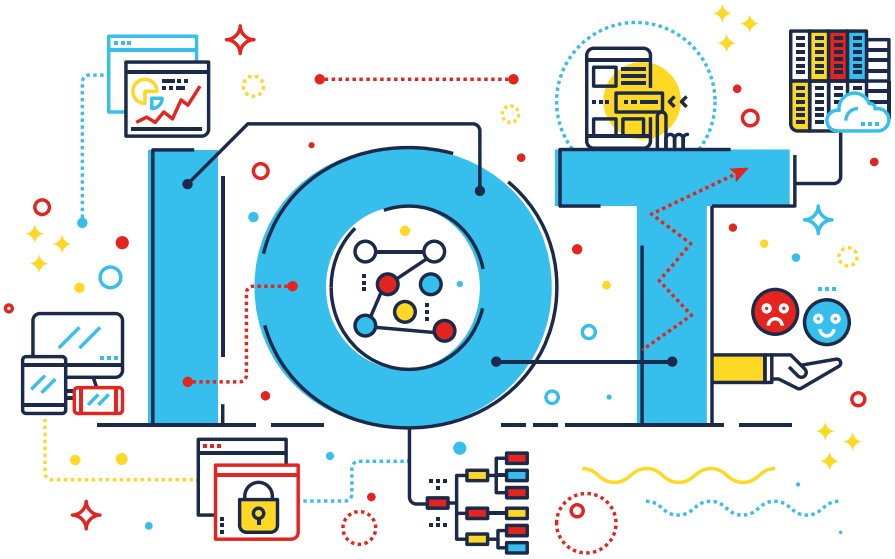
(1) http://www.basvankaam.com/2017/04/04/iot-use-case-the-connected-cow-yes-really/

(2) https://connected.messefrankfurt.com/2016/04/08/the-internet-of-things-not-new-but-more-important-than-ever/

/// LA QUESTION DE L'IDENTIFICATION DANS L'IOT

En poursuivant avec l'exemple de la vache présenté plus haut, l'éleveur doit identifier une vache donnée dans son troupeau. À cet effet, le podomètre apposé sur chaque vache doit être associé à un identifiant unique. Dans ce cas, la portée de l'unicité des identificateurs peut se limiter au troupeau uniquement.

L'IoT a néanmoins pour vocation de connecter des milliards d'appareils à l'Internet. L'identifiant de chaque objet doit donc être unique dans cet espace. Dans l'infrastructure Internet actuelle, l'identification unique d'un objet (un ordinateur ou un routeur étant également un « objet » au sens de l'IoT) repose sur son adresse IP (IPv4 ou IPv6). Les adresses IP respectent une convention de **nommage** spécifique [3]. Il existe une structure hiérarchique [4] qui fournit l'adresse IP, et garantit l'unicité (en d'autres termes, deux périphériques identifiés sur Internet ne peuvent pas avoir la même adresse IP). Il arrive que certains objets n'utilisent pas le système mondial d'adressage IP, mais une adresse IP privée. Les objets associés à une adresse privée sont malgré tout connectés à Internet à l'aide d'un dispositif passerelle qui utilise une adresse IP mondiale pour transporter les données du réseau privé vers l'Internet, et vice versa.



Comme mentionné plus haut, l'IoT peut englober des dispositifs non-IP ; par conséquent, ceux-ci ne sont pas identifiés à l'aide d'adresses IP. Leur mode d'identification varie selon qu'il s'agit de dispositifs anciens (legacy) ou de dispositifs plus récents. Bien avant l'avènement du concept d'IoT, il existait déjà pour les dispositifs des conventions de nommage et une structure permettant de transmettre les identifiants aux utilisateurs finaux. Ces identifiants anciens vont de EUI-48 et EUI-64 pour les adresses MAC, aux identifiants d'objets numériques (DoI) pour les contenus électroniques, en passant par le code produit électronique (EPC) pour les étiquettes RFID, les codes à barres, etc. Les identifiants récents obéissent à des conventions de nommage nouvelles et disposent d'une structure dédiée pour leur transmission, conçue en réponse aux besoins particuliers de chaque segment de l'industrie IoT.

Pour résoudre les problèmes posés par la disparité des conventions de nommage, un scénario serait qu'un organisme de normalisation élabore une convention de nommage à portée mondiale (convention unique), universelle, et demande à tous les acteurs de l'écosystème IoT, qu'ils soient anciens ou récents, de migrer vers cette convention harmonisée. Grâce à la standardisation des protocoles tels que IPv6 et aux avantages associés à un vaste espace d'adressage, c'est aujourd'hui possible.

Dans la pratique, toutefois, au vu de notre expérience acquise auprès des acteurs du secteur de la chaîne d'approvisionnement (qui utilisent les technologies RFID et codes à barres) par exemple, nous [5] estimons qu'il sera presque impossible d'appliquer une seule et même convention de nommage mondiale à tous les « objets ». Certains secteurs tels que les produits de consommation, l'automobile ou la défense utilisent depuis longtemps leurs propres conventions de nommage. Dans ce contexte, la migration vers une convention de nommage mondiale pour l'identification des objets ne semble pas une solution réalisable compte tenu de son lourd impact sur les infrastructures des acteurs concernés. À titre d'exemple, il nous semble peu probable voire impossible d'imaginer Walmart et Carrefour abandonner les codes à barres et utiliser des adresses IPv6 pour étiqueter leurs produits...

(3) https://en.wikipedia.org/wiki/Naming_convention

(4) https://tools.ietf.org/html/rfc2050

(5) «notre» ou «nous» instances dans cet article représente Afnic

/// SERVICE DE NOMMAGE

Compte tenu de l'hétérogénéité des conventions de nommage, des identifiants et des structures d'approvisionnement, la question qui se pose est la suivante : sera-t-il possible de communiquer entre des « objets » qui utilisent différentes conventions de nommage d'identifiants ?

Deux approches sont envisageables : une approche dite « de rupture »[6] (*disruptive approach*) ou une approche dite de continuité (*evolutionary approach*). S'agissant de l'IoT, il existe un certain nombre d'approches de rupture . La plupart d'entre elles émanent du milieu universitaire ; elles ont été mises en œuvre en environnement de laboratoire (ou) testées dans des cas d'utilisation spécifiques.

L'approche évolutive consiste à utiliser les technologies existantes et ayant fait leur preuve face aux contraintes opérationnelles de l'Internet. Parmi ces technologies, le Service de noms de domaine (DNS), qui existe depuis le début de l'Internet et dont il reste la pierre angulaire est un candidat à prendre en considération. Bien que l'Internet ait évolué au-delà de toutes les espérances, le DNS demeure l'infrastructure de base pour la résolution d'informations sur Internet.

À l'origine, le DNS a été conçu pour traduire les noms d'hôtes conviviaux des ordinateurs connectés à un réseau TCP/IP en adresses IP lisibles par ordinateur. Outre la traduction des noms d'hôtes en adresses IP, le DNS est utilisé par exemple par les serveurs de messagerie pour déterminer où livrer les messages destinés à une adresse particulière, comme moyen général de localisation de services dans un domaine à l'aide des enregistrements SRV, pour la résolution d'identifiants sans composants hôtes traditionnels au moyen des enregistrements de ressources NAPTR, etc.

Pour l'IoT, il existe déjà des mécanismes de jonction tels que l'ONS [7] (Service de nommage des objets) et l'ODS [8] (Service de répertoire des objets) qui utilisent l'infrastructure DNS pour rattacher les identifiants dans l'IoT (à l'aide conventions de nommage existant) aux informations numériques associées sur Internet..

/// RÔLE JOUÉ PAR NOUS DANS LA PROMOTION DE L'UTILISATION DU DNS POUR L'IOT

Nous avons commencé à nous intéresser à l'IoT fin 2008, après la conférence de Nice intitulée « Internet des objets, Internet du futur », durant laquelle a été évoquée la possibilité de jeter les bases d'un « Internet du futur ».

Les discussions ont porté sur l'ONS, un service mondial de recherche qui exploite le DNS pour rattacher une étiquette RFID aux informations associées sur Internet. Selon le standard ONS V.1.0. [9], une seule zone racine de l'ONS (*onsepc.com*) gérée par Verisign Inc. contient l'intégralité de l'espace de nommage de l'ONS. Sous cette racine unique de l'ONS, un système de délégation à plusieurs niveaux pourrait être mis en place pour différents pays afin d'assurer la distribution de l'ensemble de la base de données de l'ONS.

Les questions politiques et techniques soulevées par le scénario d'une zone racine unique ont déjà été rencontrées dans le cas du DNS [10]. Les gouvernements européens (en particulier la France et l'Allemagne) ont insisté sur la nécessité d'une architecture ONS distribuée - en d'autres termes, d'un ensemble de zones racines ONS géographiquement dispersées, dont chacune est dotée d'une compétence exclusive et de fonctionnalités équivalentes à celles de ses homologues.

(6) Named Data Networking A promising architecture for the Internet of things (IoT) (https://hal.archives-ouvertes.fr/hal-01575110/document)
(7) https://en.wikipedia.org/wiki/Object_Naming_Service
(8) http://www.itfind.or.kr/Report01/200611//TTA/TTA-0079/TTA-0079.pdf
(9) https://www.gs1.org/sites/default/files/docs/epc/ons_1_0_1-standard-20080529.pdf
(10) https://www.theguardian.com/technology/2016/oct/04/us-government-internet-control-iana-address-book

Nous avons formulé la proposition d'une architecture baptisée « ONS fédéré » (F-ONS) ou « ONS multi-racines[11] », dans lequel chacune des racines homologues de l'ONS (ONS Peer Roots / OPR) serait gérée par un organisme compétent au plan suprarégional (à l'échelle d'un continent, par ex.). Sous la racine, les zones du DNS seraient déléguées à des organismes nationaux ou locaux (les zones pourraient par ex. concerner un pays dans son ensemble, une seule entreprise ou encore un consortium d'entreprises).

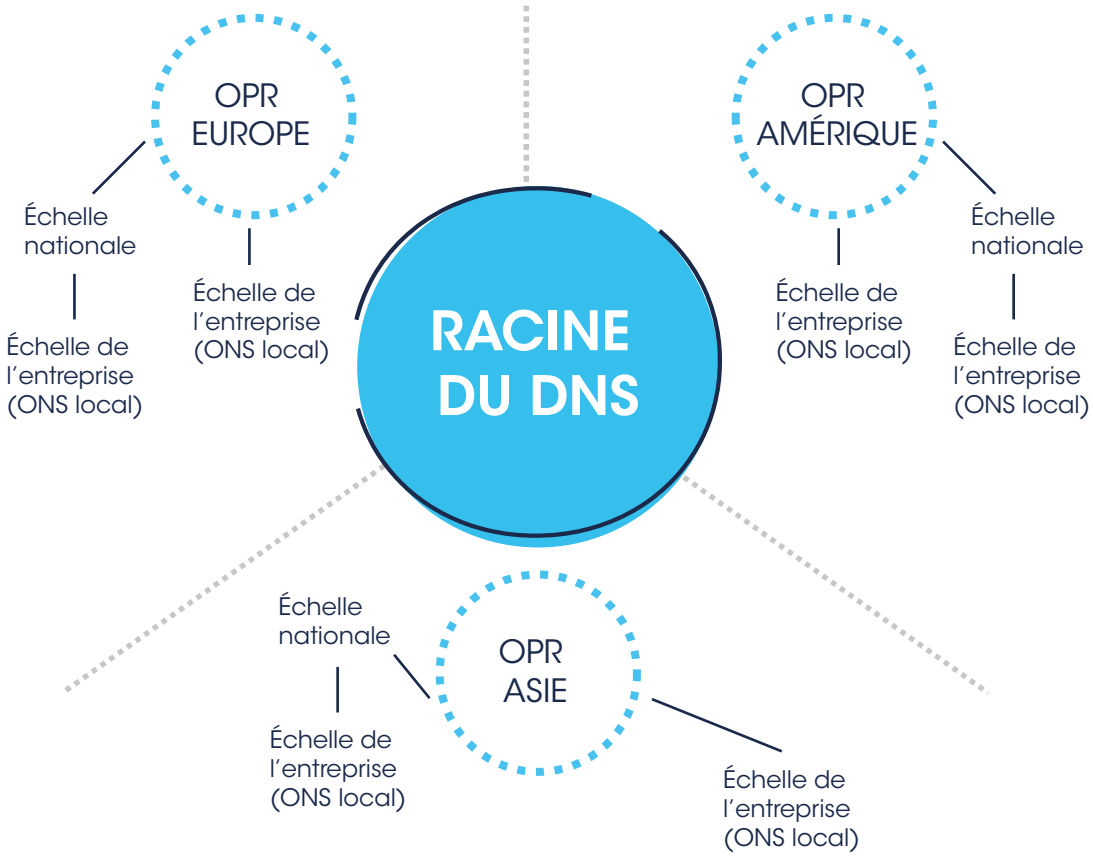


Figure 2 : Architecture « ONS Fédéré » proposée par nous

Dans le cadre du projet « WINGS » [12] de l'Agence nationale de la recherche (ANR), nous avons mis en œuvre l'architecture proposée (Figure 2) avec trois OPR : **ons-peer.eu** pour la zone Europe, **ons-peer.asia** pour la zone Asie et **ons-peer.com** pour la zone Amérique. Les délégations opérées sous chaque OPR confirment l'architecture présentée au paragraphe précédent.

La plateforme proposée offre l'avantage de la flexibilité, en ce que les entreprises d'un pays qui n'est pas en mesure de gérer son propre espace de nommage peuvent obtenir une délégation directement depuis leur OPR suprarégionale (tel qu'illustré dans la Figure 2). S'il existe une délégation de niveau national pour un pays, toutes les entreprises associées à l'Organisation membre (MO) [13] de GS1 dans ce pays doivent obtenir leur délégation depuis leur zone de niveau national.

(11) Sandoche Balakrichenan, Antonio Kin-Foo, Mohsen Souissi, "Qualitative Evaluation of a Proposed Federated Object Naming Service Architecture", Compte rendu de la Conférence internationale de 2011 sur l'Internet des objets et de CPSCom 2011, 4ème conférence internationale sur l'informatique cyber, physique et sociale, p.726-732, 19-22 octobre 2011

(12) http://www.wings-project.fr/

(13) http://xchange.gs1.org/sites/faq/Pages/there-is-no-gs1-member-organization-in-my-country-how-can-i-apply-for-barcodes.aspx

Si un pays ne souhaite pas relever d'une OPR suprarégionale, il peut disposer de sa propre OPR de niveau national ; dans ce cas, toutes les entreprises associées à la GS1 MO dans ce pays doivent obtenir leur délégation depuis leur OPR nationale. Nous avons proposé un format de requête révisé [14], , ainsi qu'une procédure de coopération entre les différentes OPR.

Nous avons également poursuivi les propositions faites dans le cadre du projet ANR-Wings avec les standards GS1[15], et toutes nos propositions ont été acceptées pour l'évolution de la norme ONS[16]. Lors de la première cérémonie des CENTR Awards 2013 [17], l'Afnic a été récompensée[18] pour ce travail.

Fin 2016, Nous avons rejoint la LoRa Alliance™[19] et avons commencé à travailler sur des compléments aux spécifications incluant l'usage du DNS dans un réseau LoRaWAN™. Conformément à la specification LoRa[20] publiée récemment (octobre 2017), le DNS doit être utilisé à différents stades de scénarios de connectivité LoRa d'un objet.

/// PRÉSENTATION SUCCINCTE DES PROBLÈMES D'IDENTIFICATION POSÉS PAR L'IOT

L'IoT pose un certain nombre de problèmes. Il ne nous est pas possible de tous les traiter dans un seul et même document. Dans cette section, nous examinerons brièvement quelques-unes des difficultés rencontrées en matière d'identification dans l'IoT. :

- **Permettre la résolution**

Il apparait donc une exigence pour l'IoT, c'est d'avoir un seul protocole pour résoudre un identifiant IoT sur Internet. Cela permettra une interopérabilité totale, quelle que soit la convention de nommage sur laquelle repose l'identifiant (existant ou émergente). Bien que définir de nouveaux standards soit une tâche chronophage et parfois fastidieuse, il nous semble important de promouvoir l'utilisation des technologies actuellement disponibles sur Internet et ne pas réinventer la roue quand cela n'est pas nécessaire.

- **Gérer l'évolutivité**

Ce protocole doit en outre être capable de prendre en charge des millions d'appareils et d'évoluer. L'une des méthodes reconnues pour assurer l'évolutivité en matière de nommage consiste à utiliser des hiérarchies de nommage de manière à limiter la portée d'un nom à une hiérarchie donnée.

- **Intégrer la sécurité**

L'un des sujets de préoccupation a trait à la sécurité des appareils connectés à l'IoT. Les attaques « IoT-centrées » [21] suscitent des inquiétudes vis-à-vis de l'adoption / du déploiement de l'IoT. Dans le cadre de la protection contre les pratiques d'exploitation de failles, les périphériques IoT doivent sécuriser leurs communications. À eux seuls, les identifiants uniques ne sont pas suffisants pour assurer la sécurité lors de la résolution des identifiants. Des mécanismes de protection supplémentaires tels que des clés cryptographiques doivent être mis en place pour prévenir les risques de falsification des identifiants.

- **Protéger les données personnelles**

Un autre sujet de préoccupation majeur s'agissant de l'IoT concerne la protection des données personnelles [22]. De toute évidence, les exigences en la matière ne peuvent être prises en compte uniquement au niveau des systèmes d'identification, le maintien de la confidentialité des données à différents niveaux étant une nécessité absolue. La principale difficulté posée par les systèmes d'identification axés sur la protection des données personnelles est que ces systèmes doivent néanmoins permettre de relier les informations provenant d'un ensemble de dispositifs à une personne ou un groupe de personnes donné(e).

(14) S. Balakrichenan, A. Kin-Foo et M. Souissi, "Qualitative Evaluation of a Proposed Federated Object Naming Service Architecture", Compte rendu de la Conférence internationale de 2011 sur l'Internet des objets (iThings/CPSCom) et de la 4ème conférence internationale sur l'informatique cyber, physique et sociale, 2011, p.726-732.

(15) https://www.gs1.org/standards

(16) https://www.gs1.org/sites/default/files/docs/epc/ons_2_0_1-standard-20130131.pdf

(17) https://www.centr.org/

(18) https://www.afnic.fr/en/about-afnic/news/general-news/7289/show/afnic-r-d-rewarded-for-its-work-on-the-internet-of-things.html

(19) https://www.lora-alliance.org/

(20) https://www.lora-alliance.org/resource-hub/lorawantm-back-end-interfaces-v10

(21) http://www.zdnet.com/article/5-nightmarish-attacks-that-show-the-risks-of-iot-security/

(22) http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=7663&no=12

/// IOT : NOTRE VISION

Même s'il existe plusieurs conventions de nommage (anciennes ou émergentes) dans l'IoT, la plupart d'entre elles présentent des caractéristiques communes :

- l'attribution des noms s'effectue de manière hiérarchisée

- le contrôle est décentralisé

- le mode d'attribution garantit l'absence de doublons.

Ces caractéristiques sont similaires à celles de l'attribution et de la gestion des noms de domaine; de la sorte, l'attribution et la résolution des identifiants dans l'IoT peuvent mettre à profit l'infrastructure et les logiciels du DNS.

Face à la croissance exponentielle de l'Internet, le DNS a su se maintenir et reste à nos jours le service de nommage utilisé pour l'infrastructure Internet actuelle. Certains mécanismes de sécurité [23] [24] et de protection de la confidentialité [25] mis en œuvre dans le DNS pourraient tout à fait être réutilisés dans l'IoT.

Nous sommes convaincus que le DNS est une option sérieuse et réaliste pour la résolution des noms dans l'IoT. Cette conviction découle des travaux menés en collaboration avec l'organisme de normalisation GS1 et LoRa Alliance™ notamment. Divers autres organismes (tels que l'IETF[26], RIPE[27] ou encore l'ICANN[28]) auprès desquels où nous intervenons ont lancé des travaux visant spécifiquement l'IoT. Forte de sa solide expertise en matière de DNS, nous avons une mission de sensibiliser/contribuer à la promotion de l'interopérabilité entre des conventions de nommage hétérogènes au sein de l'IoT.

(23) https://tools.ietf.org/html/rfc6698
(24) https://tools.ietf.org/html/rfc4034
(25) https://tools.ietf.org/html/rfc7626
(26) https://trac.ietf.org/trac/int/wiki/IOTDirWiki
(27) https://www.ripe.net/participate/mail/ripe-mailing-lists/iot-wg
(28) https://www.icann.org/en/system/files/correspondence/holmes-to-icann-01feb17-en.pdf

RENSEIGNEMENTS UTILES

Contact Afnic

Afnic
Immeuble Le Stephenson
1, rue Stephenson
78180 Montigny-Le-Bretonneux
France
www.afnic.fr

Tél. : +33(0)1 39 30 83 00

@AFNIC

support@afnic.fr

mastodon.social/@afnic

afnic.fr

À propos de l'Afnic :

L'**Afnic** est le registre des noms de domaine .fr (France), .re (Île de la Réunion), .yt (Mayotte), .wf (Wallis et Futuna), .tf (Terres Australes et Antarctiques), .pm (Saint-Pierre et Miquelon).

L'**Afnic** se positionne également comme fournisseurs de solutions techniques et de services de registre. L'**Afnic** - Association Française pour le Nommage Internet en Coopération - est composée d'acteurs publics et privés : représentants des pouvoirs publics, utilisateurs et prestataires de services Internet (bureaux d'enregistrement). Elle est à but non lucratif.