IoT ARCEP

Réponse à la consultation publique

« Préparer la révolution de l'Internet des Objets – Une cartographie des enjeux »

Septembre 2016

Table des matières

1. Introduction

Dans le cadre d'un projet de rédaction du livre blanc – Préparer la révolution de l'Internet des Objets, l'Arcep ouvre une consultation publique visant à collecter les avis des acteurs du secteur. Le document est composé de deux parties :

- Un premier document intitulé « *Préparer la révolution de l'Internet des Objets – Une cartographie des enjeux* » ;
- Le second document, intitulé « *Préparer la révolution de l'Internet des Objets – Orientations pour l'Arcep* ».

Engagé depuis 2008 dans les technologies de l'Internet des Objets (IoT), l'Afnic participe à la consultation en vue de mettre à disposition son expertise acquise pour bâtir un IoT sûr et stable, ouvert aux innovations et où la communauté Internet française joue un rôle de premier plan.

1.1. Points saillants

1.1.1. Document n°1 : « Une cartographie des enjeux »

L'Afnic souhaite tout d'abord souligner l'importance des opérateurs DNS dans cette réflexion exhaustive sur **l'écosystème IoT** ;

Ainsi, répondant à la question **des infrastructures de connectivité**, l'Afnic souligne la nécessité d'élaborer et de disposer d'une infrastructure respectant des standards ouverts et assurant la connectivité et la résilience de l'IoT.

Les recherches technologiques menées par l'Afnic autour du DNS et de l'IPv6 nous amènent à considérer ces deux technologies comme **des ressources nécessaires au développement de l'IoT** , éprouvées, permettant de briser les silos d'infrastructures IoT, sans se soucier d'une problématique de pénurie d'identifiants.

Au sujet de **l'ouverture au sein de l'IoT**, nous sommes convaincus que l'intégration de dispositifs soumis à des règles communes de connectivité est la solution à l'interopérabilité au niveau de la couche communication. Elles permettront ainsi de s'affranchir des silos technologiques verticaux ne supportant pas l'interopérabilité. Au sein de l'IETF, l'Afnic a œuvré à la mise en avant de ce thème et différents groupes de travail tels que 6LoWPAN, ROLL, CoRE, 6TiSCH traitent de ce sujet aujourd'hui.

Enfin, nous sommes persuadés de l'importance de garantir la transparence dans **la sécurité et la gestion des données privées**. Ce point est un prérequis indispensable à l'adoption de l'IoT.

1.1.2. Document n°2 « Orientations pour l'Arcep »

L'Afnic émet le souhait voir l'Arcep, comme tout régulateur, jouer un rôle au sein des principales enceintes de normalisation en France et à l'étranger. Ceci afin d'y encourager les principes d'ouverture des modèles économiques, d'interopérabilité et de choix du consommateur.

2. Contributions Afnic

2.1. L'écosystème de l'Internet des Objets

Notre réponse

Parmi l'ensemble des objets connectés qui constituent l'IoT, il existe une partie non négligeable d'objets dans l'écosystème qui sont des dispositifs à vocation d'identification tel que le RFID ou les codes-barres. Ils sont, de nos jours, très utilisés, notamment dans les secteurs de la logistique pour l'approvisionnement, le stockage ou bien la grande distribution, depuis plusieurs décennies.

Les standards GS1[1] ont déjà créé des normes axées sur l'IoT[2] pour lesquels l'Afnic a été un contributeur majeur. Dans ce cadre, nous pensons que cette consultation publique sur l'IoT sera complète lorsque les dispositifs d'identifications seront pris en compte.

Par ailleurs, le Domain Name System (DNS) est une composante fondamentale de l'écosystème Internet. Divers organismes de normalisation tels que l'ITU-T[3] ou GS1 ont déjà élaborés des normes axées sur l'exigence du besoin d'inclure le DNS pour l'IoT. A ce titre, une des recommandations de la consultation publique réalisée par la commission européenne[4] sur l'IoT est d'utiliser le DNS, notamment pour la découverte de service.

Comme les opérateurs de réseaux, les opérateurs DNS font aussi partie de l'écosystème de l'IoT.

2.2. Les infrastructures de connectivité

Notre réponse

Cette section de la consultation explicite clairement les enjeux liés aux applications de l'IoT. Ces applications se présentent sous plusieurs formes et par conséquent leurs besoins en matière de réseaux sont également variés.

Ce qui nous parait important dans ce contexte est de se concentrer sur la façon de mettre à disposition de l'utilisateur une connectivité omniprésente.

Pour cette raison, il est nécessaire d'élaborer des standards et de disposer d'une infrastructure en respect avec ces standards afin d'assurer une connectivité permanente.

Par exemple, sur un réseau de type LPWAN, il est impossible de réaliser de l'itinérance entre différentes solutions : Sigfox, Lora, Qowisio, etc. Afin de permettre l'itinérance, l'utilisation du DNS nous parait indispensable. L'Afnic réalise en ce sens des travaux avec des acteurs de la communauté.

Pour information, l'alliance LoRa travaille sur l'intégration du DNS afin de permettre l'itinérance entre différents opérateurs. De même, le standard Object Name Service (ONS), auquel l'Afnic a contribué, utilise l'infrastructure DNS pour associer dynamiquement un produit associé à un RFID ou code-barres à des informations reliées dans l'Internet.

Ainsi, le DNS jouera un rôle dans l'infrastructure de connectivité de l'IoT, similaire à celui joué actuellement au sein de l'Internet.

[1] http://www.gs1.org/standards
[2] http://www.gs1.org/sites/default/files/docs/epc/ons_2_0_1-standard-20130131.pdf
[3] http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx
[4] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1750

2.3. Les ressources rares nécessaires au développement de l'Internet des Objets

Notre réponse

Notre réponse ne portera que sur l'aspect « pénurie d'identifiants ».

Il existe effectivement des silos dans ce domaine.

Par exemple, on ne peut pas utiliser un code-barres pour identifier un objet dans un réseau de type « Zigbee » ou bien encore utiliser un capteur ayant une adresse MAC pour identifier un produit de consommation courante.

Un moyen pour briser ces silos est de mettre en œuvre un système d'identification unique tel que le système d'identification IPv6. L'espace d'adressage qu'il propose (jusqu'à 2^{128} adresses disponibles), permet l'attribution d'un identifiant unique pour l'ensemble des objets de cette planète sans se soucier d'une problématique de pénurie.

Même sans utilisation d'IPv6, une caractéristique des systèmes d'identification existants est qu'ils peuvent utiliser le DNS pour leurs besoins de résolutions de services[5] [6].

Notre suggestion serait dans ce cadre de travailler sur deux axes suivants :

- l'adoption d'IPv6 par l'ensemble des acteurs de l'IoT ;
- l'élaboration d'une infrastructure permettant l'interopérabilité entre différents systèmes d'identifications.

2.4. L'ouverture au sein de l'Internet des Objets

Notre réponse

L'IoT est constitué de dispositifs, de réseaux et d'application hétérogènes.

Différents types de réseaux tels que Zigbee pour PAN, LoRa pour LPWAN sont utilisés pour connecter différents objets sur différentes applications sans interopérabilité entre ces différents réseaux.

Notre conviction est que des dispositifs aux caractéristiques contraintes doivent intégrer le protocole de communication IP ou un de ses dérivés standardisés pour communiquer. Cela devrait assurer l'interopérabilité au niveau communication.

L'IETF a pris la mesure de ce thème et différents groupes de travails[7] ont été constitués tels que 6LoWPAN, ROLL, CoRE, 6TiSCH.

Ces groupes participent à la construction d'une connectivité bout-en-bout basée sur Internet pour IoT.

Au niveau applicatif, l'utilisation du DNS permettra l'interopérabilité comme explicité précédemment dans la question 3.

[5] http://www.gs1.org/sites/default/files/docs/epc/ons_2_0_1-standard-20130131.pdf
[6] https://www.iso.org/obp/ui/#iso:std:iso-iec:29177:ed-1:v1:en
[7] https://www.internetsociety.org/publications/ietf-journal-april-2016/internet-things-standards-and-guidance-ietf

2.5. La confiance au cœur de l'Internet des Objets

Notre réponse

L'Afnic, dans son rôle actuel de tiers de confiance sur la gestion de la zone .fr, est convaincue qu'assurer la transparence sur la sécurité et la gestion des données privées est une condition nécessaire à l'adoption de l'IoT par le plus grand nombre.

Des mécanismes sont à mettre à en œuvre afin de veiller à ce qu'aucun traitement indésirable de données personnelles n'ait lieu sans que les utilisateurs soient informés du traitement, de ses fins, et des possibilités d'exercer leurs droits. Dans le même temps, les organisations réalisant les traitements de données doivent se conformer aux principes de protection de données.

L'Afnic travaille dans ce cadre à l'amélioration de la vie privée pour les utilisateurs du DNS (notamment sur la minimisation des données[8]) et est consciente de la complexité de l'applicabilité de ces principes dans un environnement IoT où les communications automatiques entre objets et applications, sans interactions et visibilités des utilisateurs finaux, seront prépondérantes.

Sur le plan technique, un cadre approprié de protection des données personnelles devrait être définit et applicable à la plus large échelle. Mondiale idéalement, européenne au minimum, afin de concilier le respect des droits des utilisateurs et la nécessaire taille de marché minimale pour encourager les investissements et les innovations.

Par conséquent, les gouvernements et les autorités de protection des données personnelles devraient participer aux travaux des organes mondiaux de standardisation et de gouvernance et les encourager à proposer des solutions.

La conséquence directe serait de veiller à ce que les concepts de « Privacy by Design » et de confidentialité des données soient applicables.

Il est à noter que le Centre National de Référence RFID[9] a déjà travaillé sur l'évaluation de l'impact de la vie privée sur les applications RFID et dispose d'un logiciel dédié à cet effet[10]

[8] https://tools.ietf.org/html/rfc7626
[9] Le CNRFID a été nommé par le Comité Européen de Normalisation (CEN) pour être l'Autorité d'Enregistrement Européenne de la norme EN 16571 concernant le processus d'évaluation d'impact des applications RFID sur la vie privée.
[10] http://rfid-pia-en16571.eu

2.6. La période de transition pour les acteurs de l'Internet des Objets

Notre réponse

Les discussions sur IoT devraient privilégier une approche techniquement neutre.

Une régulation réalisée selon des intérêts locaux est primordiale mais doit être incluse dans une régulation élargie au niveau Européen et mondial afin de ne pas ralentir l'innovation et la compétitivité globale.

L'implication de services de Recherche & Développement (R&D) est un des éléments cruciaux pour apporter une vision de l'IoT enrichie.

Les organismes publics en France ont joué un rôle important pour stimuler la R&D autour de l'IoT.

Le résultat concret est qu'un certain nombre de sociétés françaises jouant le rôle de pionniers dans l'industrie IoT sont actuellement très bien positionnés sur ce marché.

Nous pensons que cette dynamique doit être maintenue et que les efforts de recherche et leurs financements restent nécessaires pour permettre la transition et le passage de concepts R&D à des produits commerciaux avec les retombées économiques associées.

---- Fin du document ---