

Quel référentiel pour les solutions IoT ?

11 et 14 décembre 2017

Sommaire

1. Contexte

2. Le référentiel IoT

Démarche

- ❑ L'Arcep cherche à faciliter et d'accompagner l'émergence de l'Internet des objets. Cela signifie :
 - Connaître et comprendre l'écosystème
 - Identifier les éventuelles barrières réglementaires à l'auto-organisation de l'écosystème et les lever (à l'échelle européenne si possible)
 - Mais ne pas influencer sur le choix des technologies, qui doit être arbitré par le marché

- ❑ Les problématiques liées à l'IoT étant très transverses, l'Arcep s'attache à collaborer avec d'autres administrations.
 - France Stratégie, ANSSI, DGE, DGALN, ANFR, CNIL

- ❑ Plus largement, l'Arcep cherche à favoriser l'innovation dans le domaine des télécommunications et du numérique.
 - Ouverture d'un « bac à sable réglementaire » pour permettre aux sociétés intéressées de réaliser des expérimentations
 - Présence à l'incubateur de start-up Station F
 - Ouverture prochaine d'un portail des fréquences libres pour recueillir les problèmes de qualité de service dans ces bandes libres

Travaux

- ❑ Publication par l'Arcep d'un livre blanc sur l'loT en novembre 2016, basé sur un cycle d'auditions et d'ateliers préparatoires.

- ❑ Cinq principaux objectifs identifiés à l'issue du livre blanc :
 - Assurer une connectivité multiple, mobile, fiable
 - Veiller à la disponibilité des ressources rares (fréquences, identifiants)
 - Garder un jeu ouvert à tous
 - Contribuer à bâtir la confiance autour des données
 - Poursuivre le dialogue avec les acteurs de l'loT

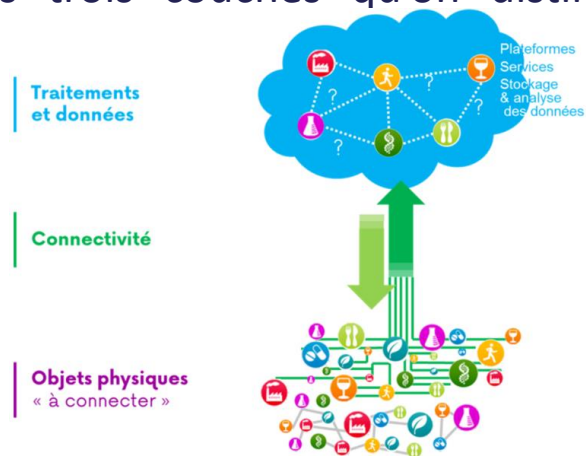
- ❑ Dans la continuité de ces travaux, l'Arcep organise deux ateliers consacrés à la réflexion autour d'un référentiel de comparaison des solutions loT.
 - Un atelier « utilisateurs » et un atelier « fournisseurs »
 - L'enjeu est de permettre à l'utilisateur de faire un choix éclairé, afin de favoriser la dynamique concurrentielle entre fournisseurs de solutions loT
 - Le référentiel proposé n'a pas vocation à être normatif dans un premier temps, mais pourrait servir à alimenter les discussions européennes

Le référentiel IoT

Le référentiel IoT

□ Le périmètre du référentiel IoT porte sur les trois couches qu'on distingue généralement :

- L'objet connecté (le terminal)
- Le réseau (la connectivité)
- La plate-forme (stockage et traitement des données)



□ Plusieurs axes de comparaison ont été pré-identifiés par l'Arcep, et sont soumis à discussion :

- Connectivité et qualité de service
- Protection des données personnelles
- Sécurité
- Consommation énergétique
- Pérennité
- Ouverture et interopérabilité

Axe 1 : la connectivité et la qualité de service

- ❑ On constate une profusion de technologies de connectivité, filaire ou sans fil, utilisant les bandes libres ou les bandes sous licence.

- ❑ La connectivité d'une solution IoT pourrait s'évaluer via les sous-critères suivants :
 - Couverture des émetteurs (zones blanches, en intérieur, sous terre, pays étrangers...)
 - Débit (maximum théorique, minimal garanti ?)
 - Taux de livraison des messages, risque de brouillage (y compris pour le futur)
 - Possibilité de bascule vers un autre protocole en cas de coupure
 - Contraintes techniques réglementaires (puissance maximum d'émission, taux d'occupation)
 - Facilité de déploiement des infrastructures, possibilité d'installer des répéteurs
 - Sobriété d'exposition aux ondes électromagnétiques

- ❑ Questions pour discussion :
 - Cet axe et ces sous-critères vous paraissent-ils pertinents pour comparer des solutions IoT ?
 - Comment les différents protocoles de communication se positionnent-ils ? (Wi-Fi, Bluetooth, 2G, 3G, 4G, NB-IoT, LTE-M...)

Axe 2 : la protection des données personnelles

- ❑ Les objets connectés peuvent transmettre et exploiter des données personnelles. L'enjeu de cet axe est double :
 - D'une part, informer clairement l'utilisateur sur le traitement de ses données personnelles
 - D'autre part, déterminer la capacité d'une solution IoT à traiter des données personnelles plus ou moins sensibles

- ❑ Cet axe pourrait être évalué via les sous-critères suivants :
 - Certification/labels prévus par le RGPD, pour distinguer les solutions IoT les plus protectrices de la vie privée
 - Suivi des recommandations des « packs de conformité » de la CNIL
 - Maîtrise par l'utilisateur du choix du responsable du traitement des données et des éventuels sous-traitants, de la localisation du stockage et du traitement des données, de l'exploitation par des tiers des données collectées
 - Capacité de l'objet à fonctionner en cas de refus par l'utilisateur de la collecte de ses données personnelles

- ❑ Questions pour discussion :
 - Cet axe et ces sous-critères vous paraissent-ils pertinents pour comparer des solutions IoT ?
 - Cet axe et ces sous-critères peuvent-ils être quantifiés facilement ?

Axe 3 : le niveau de sécurité

- ❑ Les failles de sécurité potentielles posent de véritables défis quand à la maîtrise des données, qu'elles soient personnelles ou professionnelles.

- ❑ Le niveau de sécurité permis par une solution IoT pourrait être évalué via les sous-critères suivants :
 - Certification/labels pour garantir le sérieux du prestataire (ex : labels de l'ANSSI « ESCloud » ou « SecNumCloud » pour la couche plateforme)
 - Respect des recommandations de l'ANSSI
 - Protocole de chiffrement des données
 - Présence de mécanismes d'authentification
 - Réalisation d'une analyse de risque (type EBIOS)

- ❑ Questions pour discussion :
 - Existe-t-il des labels garantissant la sécurité d'une solution IoT sur l'ensemble de la chaîne?

Axe 4 : la consommation énergétique

- ❑ La consommation énergétique peut être un critère de comparaison important, surtout lorsque l'objet connecté est situé dans une zone difficile d'accès.

- ❑ Cet axe pourrait être évalué via les sous-critères suivants :
 - La consommation d'énergie en conditions d'utilisation standard (qui peut être difficile à définir)
 - Pour les objets non raccordés au réseau électrique, l'autonomie
 - La résilience de l'objet en cas de coupure de courant (batterie intégrée, capacité à garder les données en mémoire)

- ❑ Questions pour discussion :
 - Quel compromis entre consommation énergétique et sécurité des communications ?
 - Peut-on définir des profils d'utilisation standards pour mesurer la consommation d'énergie ?

Axe 5 : la pérennité

- ❑ Le déploiement des objets connectés pourrait être entravé par le risque d'obsolescence ou de désuétude des technologies à long terme.

- ❑ Cet axe pourrait être évalué via les sous-critères suivants :
 - Durée minimale garantie de maintenance de l'objet, des technologies utilisées, de l'environnement logiciel et matériel
 - Capacité de la solution IoT à basculer vers d'autres technologies équivalentes, sans surcoût pour l'utilisateur
 - Degré de dépendance vis-à-vis d'une entreprise en particulier (opérateur mobile, entreprise déployant le réseau...)

- ❑ Questions pour discussion :
 - Cet axe et ces sous-critères vous paraissent-ils pertinents ?
 - Cet axe et ces sous-critères peuvent-ils être quantifiés facilement ?

Axe 6 : l'ouverture et l'interopérabilité (1/2)

- ❑ L'enjeu est notamment de quantifier la richesse de l'écosystème auquel l'objet connecté donne accès.
 - L'ouverture désigne l'accessibilité d'un système à l'ensemble des acteurs, au-delà de son propriétaire
 - L'interopérabilité désigne la compatibilité entre les objets et entre les applications

- ❑ Cet axe pourrait être évalué via les sous-critères suivants :
 - Capacité de l'objet connecté à basculer vers une autre technologie, vers un autre opérateur (ex : cartes SIM virtuelles) ou vers une autre plateforme
 - Capacité de l'objet à communiquer avec d'autres objets hétérogènes (de fonction différente, de marque différente), à accéder à différentes plateformes
 - Degré de portabilité des données (voire des algorithmes)
 - Degré d'ouverture des standards utilisés par les technologies de communication et d'adressage

- ❑ Questions pour discussion :
 - Cet axe et ces sous-critères vous paraissent-ils pertinents ?

Axe 6 : l'ouverture et l'interopérabilité (2/2)

- ❑ Exemples de standards de communication :
 - Standards 3GPP pour les réseaux mobiles ouverts au publics
 - Standard ouvert : toute entreprise peut librement déployer et exploiter le réseau (ex : LoRa)
 - Standard propriétaire : une entreprise contrôle le déploiement et l'exploitation du réseau, en passant éventuellement des accords avec des opérateurs partenaires (ex : Sigfox)

- ❑ Exemples de standards d'identification et d'adressage :
 - Standards ouverts : numéros de téléphone mobile, identifiants de carte SIM, adresses IP...
 - Standards propriétaires : autres formats non ouverts.

- ❑ Exemples de gouvernance au niveau des plateformes:
 - Gouvernance collective autour d'une alliance : exemple de l'Open Connectivity Foundation, qui propose un standard commun via la technologie Alljoyn, en *open source*
 - Gouvernance autour d'un acteur unique : exemple d'HomeKit pour Apple, de Weave pour Google, qui jouent le rôle de passerelle entre les objets.

Questions transverses

- ❑ Y-a-t-il d'autres axes qui devraient être inclus dans le référentiel ? Lesquels ?

- ❑ Sous quelle forme l'information devrait-elle être présentée aux utilisateurs finals ?
 - Exemple : grille de comparaison ? Étoile à plusieurs dimensions ?

Suite de l'atelier

- ❑ Un compte-rendu sera transmis aux participants pour validation, avant mise en ligne sur le site de l'Arcep consacré à l'IoT : <http://www.arcep.fr/iot/>

- ❑ De prochains ateliers sont envisagés par l'Arcep à moyen terme :
 - IoT & blockchain
 - IoT & TPE-PME : un levier de développement économique des territoires
 - IoT & smart cities : l'enjeu de l'accessibilité

Merci
de votre
participation

