SSR - Télécom SudParis 2012

Internet of Things – Privacy

Technologies, Utilisations, Problèmes de vie privée et Solutions

François-Xavier Aguessy
Côme Demoustier

Encadrant : M. Laurent

Sommaire

Introduction **3**

Partie I – Les Technologies de l'Internet of Things **4**

Les technologies d'identification 4

Code-barres *4*

GPS *4*

Carte SIM *4*

RFID *5*

Les Technologies de communication et de structuration des objets 6

Communication avec les codes-barres et architecture classique *6*

Communication RFID et architecture nouvelle *7*

Structuration des objets *8*

Protocoles indépendants en expansion *8*

Partie 2 – Utilisations de l'Internet of Things **10**

Etat de l'art de l'utilisation des technologies de l'IoT 10

Code-barres *10*

RFID *10*

NFC *10*

Zibgee *11*

Rubee *11*

Wifi et Bluetooth *11*

Utilisations futures de l'IoT 11

Un Internet des Objets domestique centralisé par un OS *11*

Une domotique intégrée à la vie courante *12*

Partie 3 – Les risques de l'Internet of Things pour la vie privée **13**

Privacy, Definition et Application 13

Risques des technologies actuelles 13

Risques sur les étiquettes RFID *14*

Risques sur le NFC *14*

Partie 4 – Solutions et Réglementation **15**

Réglementation 15

Solutions techniques pour protéger la vie privée 16

RFID *16*

NFC *16*

Solutions pour l'Internet of Things *16*

Conclusion **19**

Annexes **20**

Annexe A – Récapitulatif des technologies d'identification 20

Annexe B – Tableau des distances et des fréquences d'utilisation des tags RFID 20

Bibliographie **21**

Introduction

L'Internet of Things (IoT) ou Internet des Objets vise à créer de nouveaux réseaux de réseaux non pas dédiés aux ordinateurs clients/serveurs ou Smartphones, mais à tout élément de nos différents environnements. Les premiers objets visés ont été les éléments des chaînes logistiques dans les milieux professionnels pour optimiser la production. Nous voyons, aujourd'hui, l'introduction de tels objets connectés dans les milieux domestiques, au travers des appareils grand public, ainsi que l'avènement de la domotique pour gérer nos maisons et appartements. La mise en réseau de ces objets peut donc se faire à travers de nouvelles architectures dédiées, ou bien participer à l'évolution de l'Internet en prolongeant le réseau classique. Dans tous les cas, l'introduction de ces nouveaux objets dans le cyberespace conduit à la mise en place de nouveaux protocoles pour qu'ils puissent communiquer entre eux et avec le reste du réseau. D'autres technologies déjà existantes et qui font aujourd'hui leur preuve par leur omniprésence dans nos milieux, vont aussi être particulièrement adaptées à la vulgarisation de l'Internet des Objets.

Le premier concept de l'IoT est l'identification des objets. Elle permet en effet de faire le lien entre l'objet physique et l'objet virtuel présent sur le réseau. Le deuxième concept clé est l'importance des réseaux, c'est-à-dire les différents moyens de communication entre les objets. Enfin, la dernière notion importante de l'IoT est le traitement qui sera effectué sur les objets et les données.

Pour décrire l'IoT, nous suivrons le plan suivant : pour commencer, nous décrirons les technologies principales utilisées dans l'Internet des Objets, celles qui identifient les objets, celles qui leur permettent de communiquer et celles les structurent. Ensuite, nous verrons les utilisations actuelles de ces technologies et comment elles peuvent interagir pour donner l'IoT. Nous étudierons alors les faiblesses de ce système et quels problèmes cela peut engendrer vis-à-vis de la vie privée des utilisateurs. Enfin, nous verrons quelles solutions réglementaires ou techniques il peut y avoir pour remédier à ces problèmes.

Partie I – Les Technologies de l'Internet of Things

Les technologies d'identification

Comme nous l'avons vu dans l'introduction, la première étape nécessaire pour créer un *Internet des Objets* est d'**identifier** ces objets. Nous allons présenter ici quelques-unes des technologies d'identification les plus utilisées.

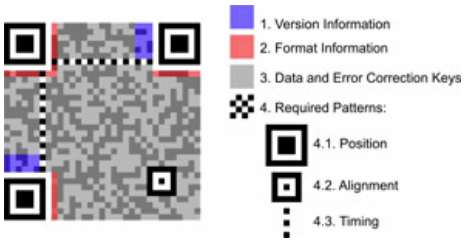
Code-barres

La première technologie qui est apparue afin d'identifier les objets est le **code-barres** [1] [2]. C'est un symbole sur fond blanc composé de barres sombres parallèles plus ou moins épaisses et séparées par un espace plus ou moins large. C'est l'épaisseur de l'espace et des barres qui permet de coder des symboles (numériques ou alphanumériques).

Un lecteur de codes-barres utilise un **composant optique** qui transforme le signal lumineux en un signal électrique : les barres sombres absorbent la lumière, alors que les barres blanches la réfléchissent. Ensuite, ce signal électrique est décodé en caractères suivant un **code** normalisé (EAN, Code 39,…). On récupère alors l'identifiant du produit scanné.

Le principal défaut des codes-barres est la limite de stockage d'informations, pour la norme EAN 13, 13 chiffres chacun codé sur 7 bits soit 91 barres élémentaires. Pour répondre à ce problème, une évolution du code-barres classique est le **code-barres à deux dimensions**. Le principe est le même, mais au lieu d'être composé de barres (une dimension), le code est composé de carrés (deux dimensions).

Les **QRCodes** [3] sont surement les code-barres à deux dimensions les plus répandus, car ils sont publiés sous licence libre. C'est un code-barres matriciel qui comporte une mire, 3 repères carrés permettant au lecteur de déterminer la dimension et l'orientation du code, ainsi que d'autres informations permettant de savoir comment le décoder (version, format,…). Un QRCode peut contenir plusieurs types d'identifiants comme un lien vers un site internet, une carte de visite virtuelle, un numéro de téléphone, des coordonnées GPS, ou un texte libre.



Le défaut qu'ont à la fois les codes-barres 1D et 2D est qu'ils sont **statiques** : une fois qu'un code-barres est imprimé, on ne peut plus ajouter aucune information dessus. Nous allons donc voir d'autres technologies qui peuvent interagir dynamiquement avec leur milieu.

GPS

Le GPS est une technologie adaptée uniquement pour **identifier des lieux**. C'est un système de géolocalisation mondial fonctionnant à l'aide de satellites américains. Il existe d'autres systèmes de positionnement par satellites qui fonctionnent de la même manière, par exemple GLONASS (Russie) et Galileo (Union Européenne). Pour se géolocaliser, une puce GPS utilise l'une ou plusieurs des constellations évoquées précédemment pour faire une trilatération et calculer sa position. Les coordonnées GPS sont des mesures qui permettent d'identifier un lieu extérieur avec précision.

Carte SIM

La carte SIM est une carte à puce constituée d'un microcontrôleur et de mémoire. Elle est présente dans presque tous les téléphones portables et permet à l'opérateur de stocker l'identifiant de l'abonné. Son organisation en répertoire et en fichiers fait qu'il est possible sur certaines cartes SIM récentes de stocker d'autres données ou applications. Par exemple, la

carte SIM peut être utilisée pour stocker de manière sécurisée les données utilisées par le NFC sur mobile. La carte SIM permet donc d'identifier un téléphone. Il est possible d'ajouter dessus des informations même après sa création (car elle possède de la mémoire). C'est donc une technologie d'identification dynamique.

RFID

Les étiquettes **RFID** [4] (Radio Frequency Identification) sont composées d'une antenne et la plupart du temps d'une puce électronique qui sont toutes deux encapsulées dans une étiquette :

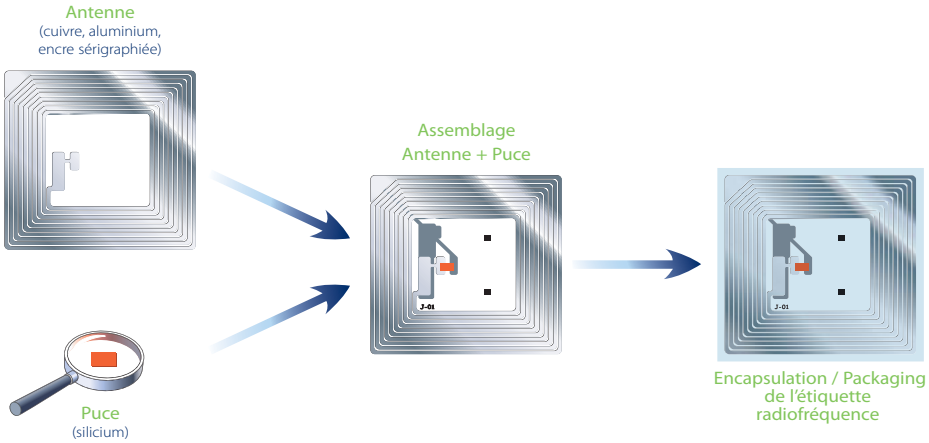


Figure 1 – Conception d'un tag RFID [4]

Il existe un grand nombre de paramètres sur lesquels les étiquettes RFID peuvent varier :

- **L'alimentation électrique** : les *tags passifs* (les plus répandus) ne possèdent pas de source d'énergie. C'est le lecteur qui leur fournit l'énergie nécessaire à la communication. Au contraire, les *tags actifs* sont équipés d'une batterie. Cela leur permet d'avoir une portée supérieure, ou de pouvoir communiquer régulièrement avec un capteur.
- Les **fréquences utilisées** : Les étiquettes RFID fonctionnent soit à des hautes fréquences HF (13,56 MHz) soit à des ultra hautes fréquences UHF (850-950 MHz) suivant la portée désirée.
- La **portée** : la portée peut aller du centimètre au mètre
- L'espace de stockage : certaines puces peuvent uniquement contenir un identifiant, d'autres peuvent avoir plusieurs Kb d'espace mémoire
- Les **fonctions cryptographiques** : Celles-ci peuvent être plus ou moins sophistiquées selon le niveau de sécurité désiré
- Les **opérations de lecture ou d'écriture** : Certaines étiquettes sont en lecture seule et il est uniquement possible de lire le numéro d'identification défini par le fondeur. D'autres peuvent être écrites une seule fois à leur activation puis lues plusieurs fois. Certains tags ont des pages de mémoires réinscriptibles à volonté.

En fonction de tous ces paramètres, les étiquettes RFID ont un coût qui peut aller de 0.30 à 100 €.

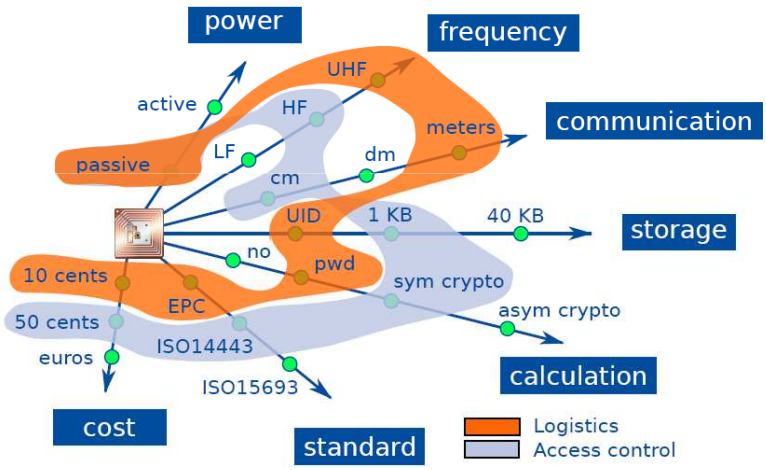


Figure 2 – Les différents types de tags RFID [5]

Il existe encore bien d'autres techniques d'identification, comme la **technologie à onde acoustique de surface** (Surface Acoustic Wave) qui permet de récupérer jusqu'à 128 bits de données stockées sur la surface d'un cristal à l'aide d'ondes radio. De même, **la technologie de circuits à transistors sur film fin** (Thin Film Transistors Circuits) permet de stocker 128 bits de données via des dépôts chimiques sur des films en plastiques. Nous ne verrons pas plus en détail ces techniques, car elles ne sont encore pas très répandues.

Voir récapitulatif des technologies d'identification en Annexe A.

Les technologies de communication et de structuration des objets

Des couches supérieures jusqu'au support physique, nous allons nous intéresser aux **premiers segments du réseau**, c'est-à-dire entre le cyberobjet lui-même et le 1er point d'accès qui va permettre d'introduire cet objet dans l'architecture.

Communication avec les codes-barres et architecture classique

Afin de mieux comprendre les architectures futures utilisant par exemple le NFC, revenons aux technologies de communication qui sont utilisées pour l'identification d'objets par code-barres. Comme vu dans la sous-partie précédente, la lecture de l'identité de l'objet se fait de manière **optique** (capteur CCD tel que sur les APN ou capteur laser) avec conversion du signal lumineux en signal électrique au niveau du lecteur optique. Il faut ensuite que cette information binaire soit récupérée par un ordinateur pour être traitée par le système d'information. Ainsi, l'interfaçage entre le lecteur optique et l'ordinateur peut se faire au travers de plusieurs supports physiques tels que l'interface **RS-232** ou **USB**. Ces interfaces utilisent différents protocoles de "liaisons de données" comme le protocole USB pour échanger les trames de données. L'ordinateur peut donc **traiter l'information** et récupérer toutes les caractéristiques d'un produit (prix, stock, composition...) sur le réseau en interaction avec une base de données. On peut considérer que ce couplage [lecteur optique - ordinateur] correspond à notre 1er segment d'une architecture IoT très basique.

GTIN

Global Trade Item Number: 3270190583592

Trade Item Ownership

Trade Item Info

Search

This information is provided on behalf of GS1 France.

GLN	COMPANY	CONTACT	LAST CHANGE	GCP	STATUS	PROVIDER GLN
3020470000000	CARREFOUR HYPERMARCHES FRANCE DSIG GROUPE CARREFOUR 9-13 AVE D BOIS BRIARD - COURCOURONNES 91003 EVRY CEDEX France	www.m.carrefour.fr	20.12.0404	302047	0	3027000000103

Responder: 3027000000103, Responses: 1, RC: 0 (No error)

Figure 3 – Base de données universelle du GS1 [7]

Dans cette illustration, nous avons utilisé la base universelle du GS1 pour identifier un achat. Le GS1 [6] est l'organisme mondial majeur dans les normes de codage d'identifiants [7]

Communication RFID et architecture nouvelle

Le QRCode connaît un véritable essor de nos jours. Cependant, la véritable évolution du code-barres se dessine au travers de la technologie RFID. Nous avons vu précédemment de quoi était constitué ce tag, que certains sont modifiables et que d'autres supportent l'ajout de nouvelles informations. Il s'agit ici de comprendre comment cette technologie s'intègre-t-elle dans l'Internet des Objets. Quels sont les **protocoles** et les **architectures** déployées pour tirer profit au maximum de cette évolution ?

Comme son nom l'indique, la **technologie RFID** va utiliser le support radio pour communiquer l'identifiant que le transpondeur (tag) contient. Les plus évoluées (puces actives avec possibilité de réécriture) peuvent, en plus de l'identifiant, embarquer des capteurs de mesure (ex: pression, température...). Toutes ces informations vont donc être **modulées sur les radiofréquences**. La technologie RFID englobe aussi la manière d'échanger les informations. De même qu'il existe plusieurs types de tag RFID avec des antennes et des puces différentes, il va exister de nombreux types de communications RFID. En effet, d'un point de vue physique, le spectre des fréquences utilisées peut aller de 152kHz à 5.8GHz. Le système choisi qui va déterminer la bande de fréquence utilisée devra être adapté aux contraintes environnementales, budgétaires, au débit et à la portée voulue. [8](voir Tableau des distances et des fréquences d'utilisation des tags RFID en Annexe B)

Plusieurs méthodes de modulation sont utilisables, mais la plus fréquente est la **modulation d'amplitude** (ASK) [9]. De même, au niveau du codage, les techniques classiques RZ, NRZ, Manchester sont utilisables. Pour aller plus loin dans l'étude des composants RFID, notamment des composants passifs, il est intéressant de comprendre les notions de téléalimentation et de réflexion d'ondes que nous ne pouvons détailler ici.

Au niveau supérieur, l'échange des trames RFID entre le transpondeur et la station de base peut être initialisé de deux façons:

- la méthode TTF : Tag First Talk i.e. le Transpondeur parle en premier
- la méthode RTF : Reader Talk First i.e. la station de base parle en premier

La méthode **RTF** est la plus couramment utilisée du fait que si plusieurs transpondeurs sont présents dans la zone, la station ne peut gérer plusieurs initialisations en même temps. D'autre part, dans les deux cas, des méthodes d'anticollision ont été créées pour éviter les interférences entre communications. L'une des méthodes est **l'anticollision par intervalle de temps** où chaque transpondeur est attribué à des slots temporels. Une fois que la base a détecté l'ensemble des transpondeurs présents dans la zone et qu'elle leur a attribué un slot temporel, l'échange consiste en une succession de "command-response". Chaque commande

et chaque réponse sont contenues dans une trame. Pour aller plus loin, la construction de ces trames est normalisée dans l'ISO 18000-6[10] ainsi que tout le processus de communication RFID.

Pour compléter notre premier segment de communication, la station doit communiquer avec un ordinateur et ceci peut se faire grâce à un port RS232 ou USB.

Structuration des objets

L'objet ayant le Tag RFID est donc intégré au réseau et l'ensemble des informations échangées est bien plus riche qu'avec le code-barres. L'objet peut donc interagir avec le réseau (Internet, réseau d'entreprise). L'exemple le plus concret est la mise de EPCglobal Network standardisé par le GS1 : **l'EPCIS** [11]. Celui-ci introduit de manière pratique la notion d'ONS pour la structuration des données. L'ONS, **Object Name Service** [12], correspond au DNS de l'Internet classique. Quand un Tag RFID est lu, la machine va trouver vers quel lieu, entreprise, base de données, ou fichier sont stockées toutes les informations associées à ce produit. Avec les "**Discovery services**" de l'EPC, moteurs de recherche fournissant une multitude d'informations enregistrées à propos de chaque marchandise, de chaque entreprise, usine ou magasin (et normalisées par l'EPCIS), l'ONS permet de construire une architecture d'objets complète et accessible à tous les partenaires voulus. En effet l'EPC ajoute aussi à son Internet des Objets des "Security services" permettant aux entreprises de contrôler la confidentialité de leurs objets [4-p13]. Voici un schéma résumant l'ensemble de ces technologies:

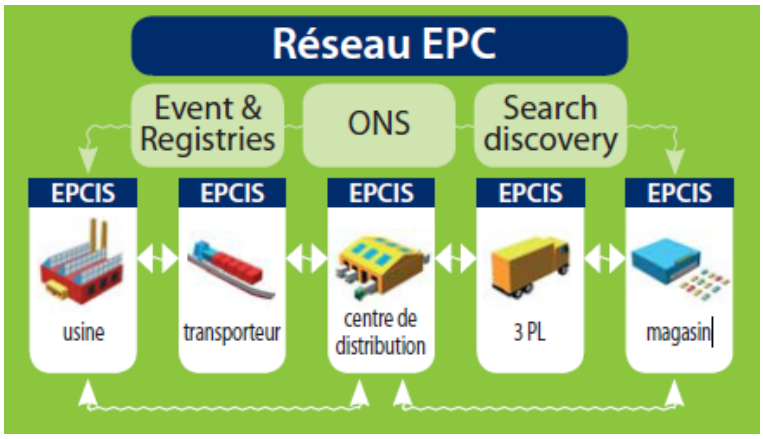


Figure 4 – Architecture de l'EPC Global network [11]

Note: la restructuration des données sur Internet est un enjeu de recherche important pour permettre des requêtes plus intelligentes. Avec les langages RDF et OWL, les données peuvent être aujourd'hui organisées sous forme d'ontologies soumises à des requêtes de recherche SPARQL. Cette structuration de données peut très bien organiser les objets d'une entreprise.

Protocoles indépendants en expansion

Enfin, d'autres technologies de communication, plus indépendantes des périphériques finaux participent grandement à l'expansion de l'IoT dans tous les environnements.

- Le **Wifi,** qui est sans doute la technologie sans-fil la plus utilisée actuellement, augmente considérablement la portée de l'IoT. Par exemple, le constructeur Broadcom développe de nouveaux modules Wifi particulièrement adaptés à l'IoT de par leur intégrations aux équipements domestiques (réfrigérateur, matériel audio et vidéo, capteurs sensoriels, voitures...). Ces modules contiennent : une antenne Wifi, un processeur, un espace mémoire pour l'exécution de programmes, une connectivité API pour

l'interface avec les développeurs et les utilisateurs. Nous verrons des exemples pratiques dans la partie "Utilisations".

- Bien que le Wifi occupe une place majoritaire dans la partie sans-fil de l'Internet, d'autres protocoles orientés Machine to Machine (M2M) prennent une place de plus en plus importante surtout grâce à leur faible consommation. La technologie **RuBee** [13] est une excellente alternative au RFID. Elle a été conçue pour être robuste dans les milieux difficiles (eau, métaux) en utilisant le champ magnétique à basse fréquence et propose une bonne autonomie (450 kHz, 10 ans d'autonomie). Bien que le débit soit plus faible que le wifi, Rubee est plus sécurisée puisque son champ d'écoute ne dépasse pas 15m. Autre technologie de plus en plus répandue : **ZigBee** [14]. Celle-ci, fonctionnant sur les ondes radio à 2,4GHz (débit 250kbs), propose de nombreuses normes de communications interopérables et adaptées à de multiples équipements. Les spécifications physiques et data-link de RuBee sont décrites dans les normes IEEE 1902.[1-2], celles de ZigBee dans l'IEEE 802.15.4.
- La technologie **NFC** (Near Field Communication) correspond à une extension de la technologie RFID à 13,56MHz et pour des échanges à moins de 10cm. Un smartphone équipé de la technologie NFC peut à la fois jouer le rôle de transpondeur et de station. Dans le rôle de la station, le mobile devient un "lecteur" d'objets environnants. Dans le rôle du transpondeur, associé à une carte SIM qui va stocker et chiffrer les données confidentielles, il devient un outil d'identification et par exemple de paiement ou un badge d'accès.

Les possibilités d'usage de ces technologies sont quasi infinies et il en existe bien d'autres (Bluetooth, Z-Wave...). De même, les architectures sont multiples, l'EPCGlobal en est une adaptée à la production à grande échelle. De nombreuses autres sont à construire notamment pour organiser les objets et les technologiques servant à la domotique (échelle domestique).

Partie 2 – Utilisations de l'Internet of Things

Nous allons voir qu'il y a actuellement de nombreuses utilisations de la plupart des technologies dont nous avons parlé. Ces technologies sont donc arrivées à une certaine maturité. Cependant, pour arriver à un véritable *IoT*, il faudrait que toutes ces technologies puissent être utilisées ensemble, c'est **l'interopérabilité des services**.

Etat de l'art de l'utilisation des technologies de l'IoT

Code-barres

Les code-barres sont utilisés pour **contrôler les flux de marchandises** depuis l'usine où ils sont fabriqués jusqu'au point de vente. Ils permettent aussi de détecter des produits contrefaits, de gérer l'état des stocks et la facturation.

Les QRCode sont eux souvent utilisés pour les **applications grand public** : tous les utilisateurs de Smartphone peuvent scanner ces codes et accéder aux informations qu'ils contiennent. Ils sont donc de plus en plus utilisés par les marques pour permettre à leurs clients d'accéder facilement à plus d'information sur un produit.

RFID

Les étiquettes RFID remplacent (ou complètent) peu à peu les code-barres pour les entreprises et ont donc les mêmes usages : **logistique**, **traçabilité des produits**… Cette technologie est particulièrement appréciée pour des usages spéciaux tels que la traçabilité dans la chaîne du froid [15] : en reliant un capteur de température à une étiquette RFID active, il est possible de mesurer la température à intervalle régulier et s'assurer que la chaîne du froid n'a pas été cassée.

Les usages du RFID sont multiples et de plus en plus nombreux : il peut être utilisé pour classer et archiver des biens, surveiller un patrimoine, assurer la sécurité des produits, faire du contrôle d'accès, tracer des animaux ou des hommes…

NFC

Le NFC est utilisé depuis longtemps au Japon, où il est souvent possible de **payer avec son téléphone portable** compatible NFC. Mais cette technologie arrive progressivement aux États-Unis ou en Europe. Par exemple à Nice où, dans le cadre du projet Cityzi [16], le NFC a été testé en condition réelle pour trois domaines différents : le **tourisme** (affichage d'informations multimédia supplémentaires à l'approche d'une étiquette RFID), les **transports** (possibilité d'utiliser son téléphone comme titre de transport) et le **commerce** (achat simplifié chez les commerçants possédant un TPE compatible).

Figure 5 - Utilisations du NFC

Une autre utilisation possible du NFC est par exemple celle effectuée par Samsung à son siège de Suwon où les badges d'accès des employés ont été remplacés par un smartphone NFC qui permettra de les identifier.

Zibgee

Le protocole de communication **Zigbee** est particulièrement utilisé pour la **domotique**, car il coûte peu cher et à une très faible consommation d'énergie. Il permet de faire communiquer sans-fil des capteurs ou télécommandes avec les équipements qu'ils contrôlent. Zigbee sert par exemple à commander une lampe, allumer une prise de courant, recevoir une alerte d'un détecteur de fumée, envoyer la température depuis un capteur tout cela sans fil.

Rubee

Le protocole Rubee peut par exemple être utilisé pour **gérer de manière sécurisée un stock** d'armes [13]. Cette gestion sécurisée peut alors comporter trois couches de sécurité :

- Chaque arme est équipée d'une puce Rubee. Les étagères où sont rangées les armes sont équipées d'un lecteur Rubee qui utilise le métal des étagères comme antenne. On peut alors vérifier en temps réel (et pour n'importe quel moment) l'état des étagères à l'aide d'un logiciel dédié
- Quand une arme est sortie d'une étagère, elle doit être marquée comme transférée à un client par un responsable munit d'un iPad qui est équipé d'un lecteur Rubee.
- Lorsqu'une arme quitte les bâtiments, une alarme est déclenchée si le porteur d'arme n'est pas autorisé à le faire et est enregistré le nom du porteur et de l'arme qui sont sortis. Cette alarme peut se déclencher même si l'arme est enfermée dans une boîte de métal, car le Rubee n'est pas perturbé par le métal.

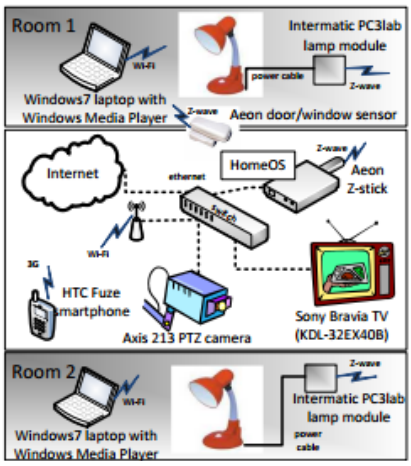
Wifi et Bluetooth

Une application du Wifi et du Bluetooth qui se rapproche beaucoup de l'IoT est l'iPavement [17], un **trottoir intelligent**. Ce trottoir, conçu par une entreprise espagnole, est constitué de dalles de béton qui ne doivent pas être éloignées les unes des autres de plus de 20 mètres pour offrir une couverture continue en Wifi et Bluetooth. Chaque dalle contient un microprocesseur et de la mémoire flash, ce qui permet, via un système de cloud computing de fournir aux utilisateurs une bibliothèque numérique, un service de musique, un catalogue de bons de réductions, des informations touristiques, mais aussi des alertes en Bluetooth aux passants et aux services publics pour les prévenir des mauvaises situations de circulation (verglas, accidents…).

Utilisations futures de l'IoT

Un Internet des Objets domestique centralisé par un OS

Si l'Internet des objets fait déjà ses preuves dans les milieux de **productions industrielles**, nous observons qu'il s'immisce de plus ne plus dans nos **environnements privés** (GPS, Wifi, Zigbee, NFC) et nous pouvons imaginer les possibilités gigantesques que possède ce système. Certaines de ces possibilités sont déjà en phase de recherche et de prototype, comme le **Microsoft Home OS**. [18]



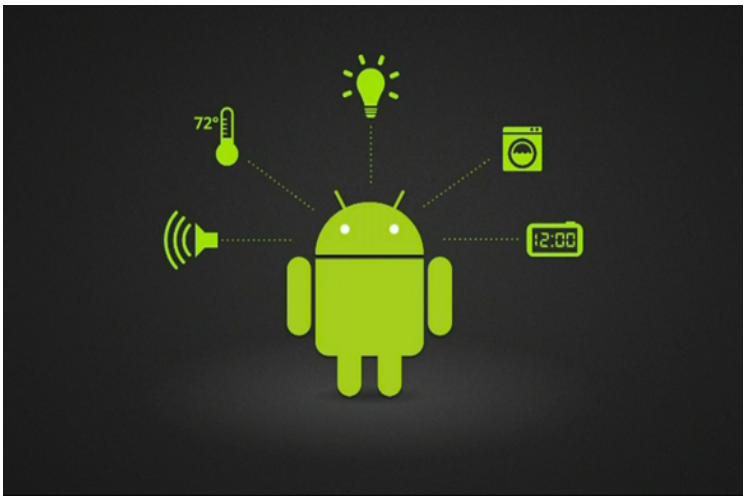
En effet, la multiplication des connectivités va nécessiter un système d'exploitation gérant l'ensemble du domaine. Microsoft va coupler avec cet HomeOS un HomeStore permettant d'installer de nouvelles

applications sur les devices voulus. Le premier exemple est un driver de Caméra IP pour PC qui redirige ensuite le flux vidéo sur Smartphone. Autre exemple, l'OS combine driver et applications de notification ainsi que des capteurs pour indiquer quelles sont les portes et les fenêtres ouvertes de la maison. Ajoutez à cela le device Kinect et vous pourrez allumer ou éteindre vos lumières par la voix ou les gestes sans quitter votre télévision.

Une domotique intégrée à la vie courante

Google se lance évidemment dans la bataille autour de son système Android. La domotique a été l'un des points dominants de la conférence Google I/O 2011 et l'Accessory Development Kit est déjà ouvert à tous les développeurs et entreprises.

Dans un futur proche, Google souhaite fournir des composants hardware pour les équipements de la maison et un ensemble d'API qui sera associé à son **Android Home Framework**. Lors de cette conférence, des démonstrations ont été faites avec des systèmes audio. Lorsqu'un CD était passé devant une chaine Hi-Fi, tous deux équipé du système NFC, l'album était copié dans la librairie musicale puis au deuxième passage, la première chanson était lancée. Une deuxième démonstration à été faite entre un téléphone Android et un vélo d'appartement. Le téléphone scanne le vélo, reconnait celui-ci, télécharge un jeu compatible et pédaler plus ou moins vite permet de contrôler des éléments du jeu. Ce projet est appelé **Android@Home**.



La vidéo de la conférence est disponible sur ce lien : [19 (minute 48)].

Partie 3 – Les risques de l'Internet of Things pour la vie privée

Privacy, Definition et Application

Proposer une définition complète de la "**Privacy**" est une tâche particulièrement difficile. En effet celle-ci peut dépendre à la fois des environnements d'utilisation (commerciale, industriel, stockage pour le grand public) et peut différer selon les pays. Nous nous permettons ici de reprendre cette phrase du rapport "IoT Architecture" de la Commission Européenne [20] : "*Privacy measures how indivdual freedom is protected, defining the zone of personal life that a person can make free of external intrusion*". À l'heure du cloud computing, il devient extrêmement délicat pour l'utilisateur de savoir où commence et où se termine cette zone de **protection personnelle**. Il faut ajouter à cela l'augmentation exponentielle des moyens de connectivité (ordinateurs portables, tablettes, smartphone, moyens de paiement, de localisation...) qui suivent à la trace l'utilisateur dans ses déplacements et son comportement. L'IoT accentue bien évidemment cette problématique puisque elle se rapporte à tout type d'objets (plus seulement à la base électronique) qui entrent en communication à la fois en zone proche de l'utilisateur et dans le cloud.

Plusieurs points apparaissent comme essentiels au niveau du respect de la Privacy dans l'Internet des Objets. Tout d'abord, l'utilisateur doit être parfaitement **mis au courant** de toutes les capacités, notamment en matière d'échange de données, dont sont capables ses appareils et applications. C'est aussi pourquoi les constructeurs ont un rôle capital à jouer dans leur investissement au sein des normes de respect de la vie privée puisque ce sont eux qui connaissent le mieux le potentiel de leur produit. De la même manière, la notion de **transparence des informations** ne doit t'être appliquée que si l'utilisateur en comprend les conditions. Enfin, plus particulièrement dans le cadre du RFID et des technologies à tag, le transpondeur doit pouvoir désactiver son identification (détruire son Tag) si l'utilisateur le souhaite.

Il est clair que toutes ces notions de *privacy* se heurtent à de nombreuses limites de notre système actuel au niveau politique, financier et comportemental. Au niveau **politique**, l'exemple le plus trivial est l'idée de Sécurité Nationale appliquée par la **rétention de données**. Celle-ci doit aussi s'élargir à l'internet des objets et surtout dans les futures utilisations du NFC comme le paiement. Au niveau **financier**, l'engouement du grand public et des entreprises pour les nouvelles technologies pousse les grands constructeurs et développeurs à augmenter le nombre de connectivités, d'introduire des capteurs sensoriels, d'adapter leurs applications à chaque profil. Or, pour créer un profil, il faut récupérer une multitude d'informations personnelles. Enfin au niveau **comportemental**, l'utilisateur n'hésite pas longtemps à sacrifier une petite part de sa vie privée pour une plus grande praticité dans sa vie quotidienne. Ce même rapport indique qu'il faudrait en moyenne 20h par mois pour lire les conditions d'utilisation de toutes les applications s'appuyant sur la collecte de données sur Internet.

Nous allons maintenant voir quels sont les risques encourus par la privacy dans l'Internet des Objets et quelques attaques qui peuvent se transposer dans l'IoT.

Risques des technologies actuelles

Les principaux risques liés à la vie privée des technologies utilisées dans l'IoT sont dus au fait que celles-ci utilisent souvent des protocoles de communication sans fil. Elles sont donc particulièrement vulnérables aux écoutes, aux divulgations d'information, à la traçabilité malveillante ou à l'altération de données. Néanmoins, l'Internet des Objets est sensé être connecté à Internet, donc toutes les menaces classiques existant sur Internet peuvent être retrouvées

sur l'IoT (redirections frauduleuses, interceptions de données…). Nous verrons dans cette partie qu'aux vulnérabilités spécialement présentes sur l'IoT.

Risques sur les étiquettes RFID

Le premier risque majeur de la technologie RFID est la **divulgation d'information** [21][22]. En effet, il est très dangereux pour la vie privée que n'importe qui puisse, s'il possède un lecteur RFID, interroger une étiquette ne lui appartenant pas. Les informations divulguées par ce tag peuvent contenir soit des informations sur l'objet contenant la puce (et donc sur son propriétaire) soit des données à caractère personnel et doivent donc être protégées.

Le second risque important pour les étiquettes RFID est le **clonage**. Cela consiste à pouvoir dupliquer une puce à partir de la puce originale. Ceci met en danger la vie privée, car les puces RFID peuvent servir pour le contrôle d'accès. Posséder une puce « clone » peut donc permettre d'atteindre des informations potentiellement confidentielles.

Enfin, les étiquettes RFID sont aussi sensibles à la **traçabilité malveillante**. En effet, même s'il n'est pas possible de savoir de quel objet il s'agit, récupérer l'identifiant de l'étiquette RFID permet aussi de tracer cet objet, c'est à dire de pouvoir le reconnaître dans des lieux différents ou a des instants différents.

Risques sur le NFC

En plus d'être sensible à la plupart des attaques possibles sur le RFID, le NFC est aussi vulnérable à des attaques spécifiques [23]. Le fait que les appareils NFC puissent interagir avec les données sécurisées comme les comptes bancaires ou des informations personnelles, fait qu'ils sont particulièrement sensibles et dommageable pour l'utilisateur.

Un appareil NFC exécute les informations qui lui sont envoyées par celui avec qui il communique. Si l'application d'exécution est vulnérable, l'attaquant pourra potentiellement gagner des privilèges et effectuer ce qu'il veut sur l'appareil.

Certaines fonctionnalités du NFC peuvent être aussi sensibles au **phishing**. En effet, au lieu que l'utilisateur compose lui-même un numéro de téléphone ou une adresse internet, celui-ci aura juste à s'approcher d'une puce. Celle-ci (ou une puce malveillante à proximité) pourra alors par exemple rediriger vers un site malveillant.

Enfin, le dernier problème spécifique au NFC est qu'il tourne souvent sur un périphérique sensible aux **virus**. De plus, comme ces périphériques peuvent dialoguer en pair à pair grâce au NFC, cela peut permettre à un virus de se répandre très rapidement.

Partie 4 – Solutions et Réglementation

Réglementation

Pour pouvoir parler de réglementation à propos de la vie privée, nous devons d'abord définir précisément les **données personnelles**. Selon la loi informatique et libertés n°78-17 du 6 janvier 1978 [24], les données personnelles sont « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* ». Cette notion représente donc toutes les données contenues avec un élément permettant d'identifier directement (comme les données nominatives) ou indirectement (via par exemple identifiant relatif à une base de données où sont stockées des données nominatives) une personne. Ceci peut donc tout à fait s'appliquer, par exemple, aux données présentes sur une puce RFID si son identifiant est mémorisé dans une base de données contenant le nom du client.

Le RFID propose des **problèmes nouveaux** par rapport aux autres types de données personnelles. Du fait que la majorité des étiquettes RFID ne possèdent pas de batterie, elles ont potentiellement une **durée de vie illimitée**, ce qui ne répond pas aux exigences de la **CNIL** sur la suppression des données personnelles une fois qu'elles ne sont plus utiles pour offrir le service proposé. Un autre problème est la possibilité **de droit de retrait** de ces informations personnelles par un utilisateur. La seule réelle solution est la destruction de la puce, opération difficile en pratique lorsqu'elle est en possession des utilisateurs. La CNIL préconise donc d'ajouter des fonctions d'**autoneutralisation** par les puces à leur production.

Pour l'instant, les problèmes nouveaux apportés par la technologie RFID ne sont pas encore pris en compte par la loi (ils restent néanmoins encadrés par la loi informatique et liberté). La CNIL [25] étudie donc actuellement ces nouveaux usages, mais n'a publié pour l'instant que des **recommandations**. Par exemple, concernant l'usage des RFID pour les transports, elle préconise que « *les données relatives aux déplacements des personnes ne soient utilisées sous une forme permettant d'identifier les usagers que dans le cadre de la lutte contre la fraude et que pendant le temps nécessaire à la détection de la fraude, ce délai ne devant pas excéder deux jours consécutifs.* »

La CNIL agit aussi pour surveiller le déploiement du NFC en France et s'assurer qu'il protège la vie privée. Son action se déroule sur 5 points clés :

- Elle s'assure que l'alias – le numéro unique fourni au fournisseur d'application (par exemple une banque) par l'opérateur – est différent pour chaque fournisseur afin qu'ils ne puissent pas faire de **recoupement d'information**.
- La CNIL fait aussi vérifier chaque application basée sur le NFC par des sociétés extérieures afin de s'assurer de la **sécurité des informations**
- Elle contrôle les applications afin de s'assurer que les **règles de confidentialité** de l'AFSCM (Association française du sans-contact) sont respectées
- Elle s'assure du **chiffrement des données** en transit lorsqu'il s'agit de transaction
- Elle a participé à fixer les **seuils de paiement** avec ou sans code et les mesures de sécurité à prendre sur l'espace sécurisé du terminal NFC

La **commission Européenne** n'a pas non plus écrit de lois spécifiques aux technologies de l'Internet des Objets. Elle a cependant publié des recommandations le 12 mai 2009 [26] sur le respect de la vie privée et la protection des données dans les applications reposant sur le RFID. Ces recommandations énoncent les 4 principes suivants [27]:

- Les consommateurs doivent être propriétaires de ce qu'ils achètent. Si un produit contient une puce RFID, celle-ci doit être **désactivée automatiquement** et gratuitement par le vendeur, sauf si le consommateur demande à ce qu'elle reste active

- Les consommateurs doivent être **informés clairement des données personnelles** qui seront utilisées via des puces et des usages qu'auront ces données
- Les produits contenant d'une puce RFID doivent être **clairement identifiés** par un sigle européen permettant aux consommateurs de les repérer
- Avant de mettre en production un produit contenant une puce, les entreprises ou pouvoirs publics doivent faire **évaluer l'incidence que ce produit aura sur la vie privée** et les données personnelles par les autorités compétentes dans leur pays.

Solutions techniques pour protéger la vie privée

Pour remédier aux problèmes de sécurités évoqués dans la partie précédente, les constructeurs ont du mettre en place des solutions pour protéger la vie privée des utilisateurs. Nous allons voir quelques-unes de ces solutions. Bien entendu, celles-ci sont **complémentaires** des protections habituelles protégeant la connexion à Internet (authentification et confidentialité par exemple via SSL).

RFID

Pour se protéger de la divulgation d'information, il a fallu ajouter des fonctions cryptographiques sur les puces RFID (ce qui a pour conséquence d'en augmenter le cout). En utilisant des fonctions de cryptographie symétrique, il est alors possible pour la puce **d'authentifier** le lecteur et pour le lecteur d'authentifier la puce si ceux-ci possèdent un secret partagé. Il faut ensuite **chiffrer** la communication entre les deux périphériques pour éviter l'écoute d'information.

Il y a plusieurs méthodes permettant de détecter les puces RFID clonées [28]. L'une d'elles est de maintenir **synchronisé** (du côté de la puce et du lecteur) **un nombre secret** dont le nombre secret pour la communication suivante est négocié à chaque fois qu'il y a une communication entre les deux. Cependant, s'il y a plusieurs lecteurs, ils devront communiquer entre eux afin de partager les secrets permettant de communiquer avec la puce.

La traçabilité peut être évitée si on ajoute un générateur de **nombre pseudoaléatoire** à la puce RFID. Celle-ci sera alors capable de répondre un résultat différent pour s'authentifier, même si elle a reçu deux fois le même message. Toutefois, là encore ceci augmente le coût de la puce et n'est donc utilisé que quand c'est vraiment nécessaire.

NFC

On peut s'apercevoir que la partie la plus vulnérable est le **terminal** support du NFC. La première solution indispensable est de bien sécuriser ce terminal afin de limiter les attaques possibles. Pour renforcer la sécurité, on peut aussi ajouter des contrôles nécessaires au niveau de la puce sécurisée : dès que les informations en jeux sont vraiment critiques (informations confidentielles, achat d'une valeur importante) il faut imposer la demande de confirmation de l'utilisateur via un code que seul lui connaît.

Il faut aussi veiller à protéger particulièrement toute la partie qui exécute les informations envoyées par un autre périphérique NFC afin de ne pas se faire infecter par un autre utilisateur.

Solutions pour l'Internet of Things

L'objectif premier des réflexions à propos de la sécurité dans l'Internet des Objets n'est pas de cloisonner ou limiter son utilisation, mais au contraire de **favoriser son évolution** dans un cadre respectueux de la vie privée. Il n'est alors pas question d'imposer telle ou telle technologie, car la richesse de l'Internet des Objets est fondée sur **l'interopérabilité** des technologies et des services.

Confidentialité, Intégrité et Disponibilité resteront les maîtres mots pour la sécurité de l'Internet des objets. Au niveau de la conception d'un Framework sécurisé pour l'Architecture de l'IoT, cinq composants ont été dégagés [29]:

- L'**autorisation** : fournir un contrôle d'accès sur l'architecture et les services
- L'**authentification** : mettre en œuvre des moyens pour vérifier l'identité des utilisateurs et des objets
- L'"**Identity Management**": pouvoir vérifier l'identité de l'utilisateur sans pour autant dévoiler toutes les informations le concernant quand celles-ci ne sont pas nécessaires au service utilisé
- La **gestion et l'échange de clés** : fournir des moyens de chiffrement pour la confidentialité et l'intégrité
- La **confiance et la réputation** : noter les éléments d'une architecture comme des capteurs quant à leur capacité à communiquer des informations sans perte d'intégrité, de confidentialité, à présenter une forte robustesse...

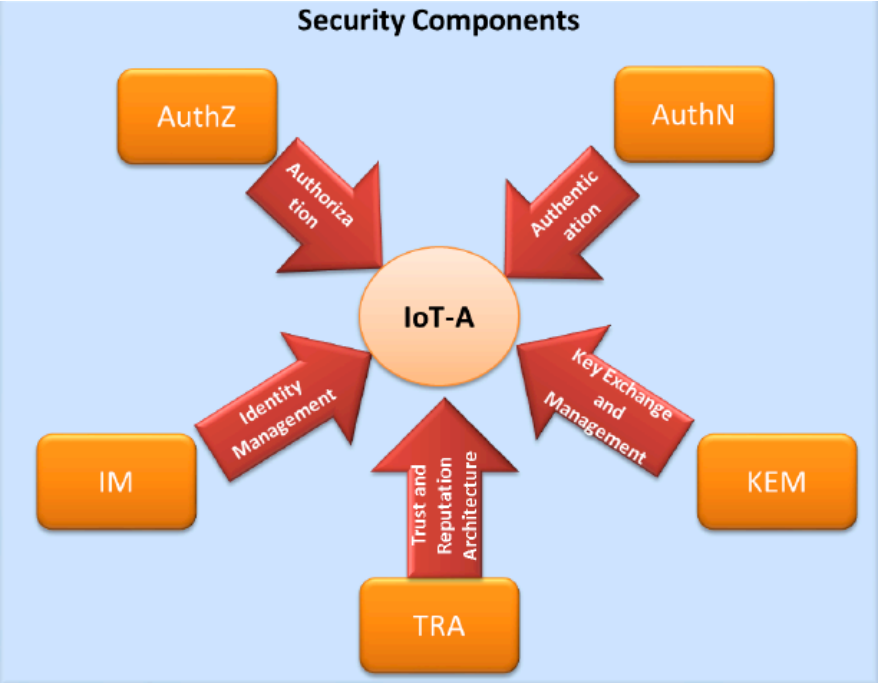


Figure 6 – Les cinq composantes de sécurité de l'Internet of Things

Chacun de ces concepts est important pour le respect de la vie privée. L'Internet classique a fortement fait évoluer les moyens de contrôles d'accès et d'authentification. L'Internet des Objets va accentuer l'importance de la gestion de son identité au sein de ce nouvel espace. Imaginons une infrastructure qui proposerait à l'utilisateur final, au sein d'une seule puce RFID, la convergence de services variés : paiement, carte de transport, passeport numérique voire carnet de santé numérique. Il parait évident que selon le lecteur RFID utilisé, dans un aéroport, un magasin ou un hôpital, le tag RFID ne devra pas donner accès à la même information, à la même identité. Le Seventh Framework Programme dans son travail avec la Commission Européenne propose le concept de "pool" d'identités. Dans ce cadre-là, chaque utilisateur ou objet présente une identité racine possédant le plus haut niveau d'information. La

puce doit ensuite pouvoir fournir des identités "enfants" possédant un degré moindre et adapté à l'utilisation pour aller chercher uniquement les informations nécessaires. L'objet devrait aussi pouvoir utiliser des pseudonymes temporaires pour des échanges anonymes.

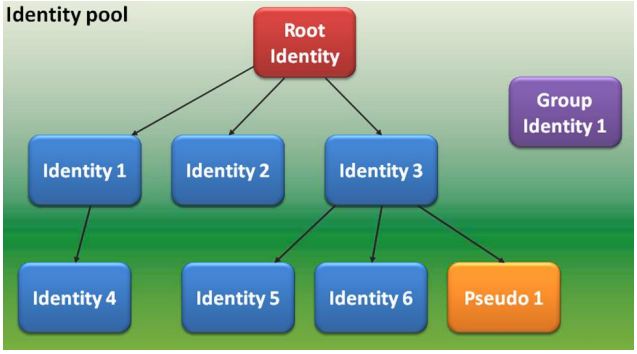
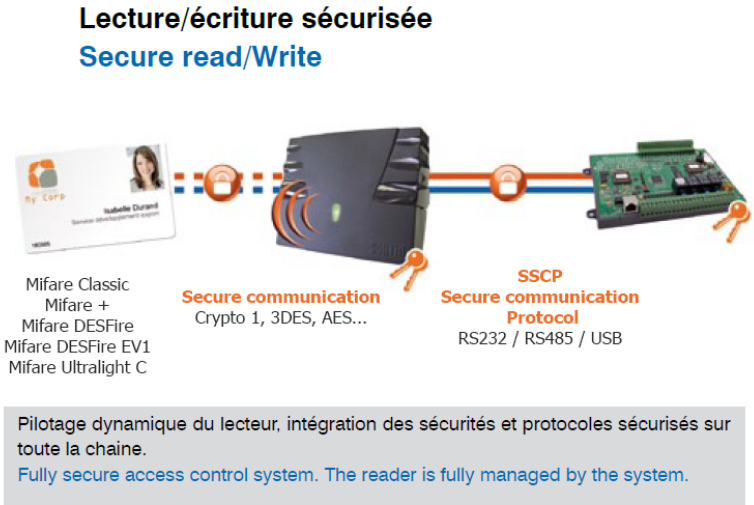


Figure 7 – Identity pool

D'un point de vu plus concret et pour le respect de l'intégrité et de la confidentialité, la mise en place d'une classification permet de connaitre les possibilités de calcul et de chiffrement d'une puce. Les puces de classe 2 (passive) permettent le chiffrement symétrique alors que les puces de classe 3 et 4, qui proposent une source d'alimentation, permettent le chiffrement asymétrique. Prenons l'exemple du constructeur français STid [30]. Il propose de nombreuses solutions de sécurité pour l'identification sans contact (santé, industrie, transport, agroalimentaire, aéronautique...). Leurs lecteurs utilisent les algorithmes 3DES, AES et RSA avec le transpondeur d'un côté, et l'algorithme AES avec le système de gestion de l'autre côté. Leur catalogue présente de nombreuses solutions de lecteurs et de Tags (carte, jeton...) adaptés aux environnements et aux besoins.



Il est aussi important de rappeler que la distance d'utilisation des tags d'identification joue un rôle important dans l'aspect sécurité de ces systèmes. Par exemple, la technologie RuBee utilise cet argument pour promouvoir son utilisation : l'utilisation du champ magnétique doit se faire à moins de 15 m de l'émetteur. De même pour le NFC qui utilise le champ électrique qui n'est possible que dans un champ inférieur à 10cm et diminue ainsi le risque d'écoute.

Conclusion

Nous avons vu que l'Internet des Objets rassemble de nombreuses technologies complémentaires et propose une multitude de possibilités. C'est là le grand enjeu de l'IoT : atteindre une interopérabilité parfaite entre tous ces services.

Les utilisations sont d'ores et déjà multiples, en particulier dans les environnements professionnels : identification, stockage et traçabilité des produits. Cependant, le marché n'en est qu'à ses débuts et les attentes en matière d'IoT dans les milieux domestiques sont considérables. Il est prévu que le marché de la technologie RFID double d'ici 2015 pour atteindre 13 milliards de dollars. Ce chiffre comprend les composants RFID, les architectures de communication ainsi que le marketing.

La concurrence et les enjeux financiers font généralement avancer plus rapidement les technologies que la réglementation et la normalisation. En effet, les constructeurs, les opérateurs et les organisations gouvernementales doivent trouver des compromis pour s'entendre à propos des nouveaux standards. C'est l'une des raisons pour laquelle la protection de la vie privée des utilisateurs est souvent en recul par rapport à l'évolution technologique. Avec l'Internet of Things, ce phénomène est accentué, car le nombre de connectivités est la quantité de données personnelles échangées sont considérablement augmentés.

Les solutions telles que les mécanismes de protection par chiffrement que l'on retrouvait sur l'Internet classique s'appliquent à l'IoT mais ils ne sont pas suffisants. Les risques d'attaques « traditionnelles » sont transposés dans l'Internet des Objets, mais l'importance de l'information contenue impose de nouvelles réflexions à propos de l'identité numérique.

L'internet des Objets promet des utilisations futures véritablement innovantes comme nous le laissent imaginer les concepts domotiques chez Google et Microsoft.

Annexes

Annexe A – Récapitulatif des technologies d'identification

Technologie	Code-barres	QR Code	GPS	Carte SIM	RFID
Identifiant	Code alphanumérique	Code alphanumérique, Coordonnées GPS, URL, Carte de visite	Coordonnées GPS	IMSI	Code alphanumérique
Réinscriptible	Non	Non	-	Oui	Oui
Coût de production	Très faible	Très faible	~1$		0.30-100€
Lecture multiple simultanée	Non	Non	Oui	Non	Oui
Type de liason	Optique	Optique	Radio	Contact	Radio
Solidité	Faible	Faible	Moyenne	Moyenne	Forte

Annexe B – Tableau des distances et des fréquences d'utilisation des tags RFID

Bande	LF	HF	UHF	UHF (haute) et SHF
Fréquences	125 kHz à 133 kHz	3,25 MHz, 8.2 MHz et 13.56 MHz	440 MHz, 860 à 960 MHz	2.45 GHz, et 5.8 GHz
Type de couplage	Inductif	Inductif	Radiatif	Radiatif
Distance d'utilisation maximale en télé-alimentation	2 à 3 mètres	1 à 5 mètres	<12 mètres USA <6 mètres Europe	<2.30 mètres USA <0.81 mètres Europe
Limites de fonctionnement	Peu sensible aux perturbations électro-magnétiques industrielles	Faiblement sensible aux perturbations électro-magnétiques industrielles	Sensible aux perturbations électro-magnétiques. Peut être perturbé par les autres systèmes UHF à proximité	Fortement sensible aux perturbations électro-magnétiques réfléchies par le métal et absorbées par l'eau

Bibliographie

[1] http://www.atscan.fr/atscan-le-guide-du-code-barre-2.asp
[2] http://atscan.com/atscan-le-guide-du-code-barre-3.asp
[3] http://www.qrmobile.fr/specificites-techniques-qrcodes.htm
[4] http://www.gs1.fr/gs1_fr/content/download/39142/363078/file/Familiarisez%20vous%20avec%20la%20RFID.pdf → « Familiarisez vous avec la RFID »
[5] Les Nouveaux enjeux de la Sécurité, 2012, Xavier Aghina, Orange Labs
[6] http://www.gs1.fr
[7] http://gepir.gs1.org/v32/xx/gtin.aspx?Lang=en-US
[8] Etat de l'art et applications des RFID, 2008, Frédéric LETIENT
[9] http://www-igm.univ-mlv.fr/~dr/XPOSE2007/mmadegar_rfid/communication_introduction.html
[10] http://www.youwokeji.com.cn/down/18000-6.pdf → « ISO/IEC 18000-6 »
[11] http://www.gs1.fr/index.php/gs1_fr/standards_gs1__1/epc_rfid/publications_et_telechargement/documents_de_vulgarisation/plaquette_le_reseau_epcglobal → «Le réseau EPC global »
[12] http://www.rfidjournal.com/faq/24/114
[13] http://www.rubee.com/TLS/index.html
[14] http://zigbee.org/About/AboutTechnology/Standards.aspx
[15] http://www.filrfid.org/article-tra-abilite-dans-la-chaine-du-froid-quelles-technologies-58398319.html
[16] http://www.cityzi.fr/
[17] http://www.ipavement.com/fr/index_fr.html
[18] http://research.microsoft.com/en-us/projects/homeos/
[19] http://www.youtube.com/watch?v=OxzucwjFEEs
[20] http://www.iot-a.eu/public/public-documents/documents-1/1/1/d1.1/at_download/file → Internet of Things Architecture
[21] RFID et sécurité font-elles bon ménage, Gildas Avoine
[22] http://www.netpme.fr/nouvelles-technologies/879-rfid-respect-vie-privee.html
[23] http://www.slideshare.net/antoine_coutant/introduction-au-nfc-et-scurit-sans-contact-dans-les-mobiles
[24] http://www.cnil.fr/en-savoir-plus/textes-fondateurs/loi78-17/
[25] http://www.cnil.fr/la-cnil/nos-defis/innovation-et-expertise/internet-des-objets-et-rfid/
[26] Journal officiel de l'Union européenne - L 122/47
[27]http://www.centrenational-rfid.com/actualites/archives/reglementation/le-12-mai-2009,-la-commission-europeenne-a-adopte-une-serie-de-recommandations/theme/3/fiche/2/fr.html?numPage=1
[28] *Securing RFID systems by detecting tag cloning*, Mikko Lehtonen, Daniel Ostojic, Alexander Ilic and Florian Michahelles
[29] http://www.iot-a.eu/public/public-documents/documents-1/1/1/d4.2/at_download/file
[30] http://www.stid.com/uploads/e-pdf/index.html