

Chapitre 3 .Réseaux et détections de proximité

une vue d'ensemble :La connectivité de votre installation IoT est sans aucun doute la partie technique la plus importante dans la réussite de votre projet.

de ce choix va dépendre :

- La stabilité de la **communication entre les objets connectés** eux-mêmes,
- Leur maintenance nécessaire,
- Et la remontée des données vers vos centres d'analyse et de traitement.

Une erreur d'appréciation dans le choix du **réseau IoT** impactera le service que vous serez en mesure d'offrir à vos clients, d'un point de vue quantitatif et qualitatif.

Brève introduction aux réseaux IoT : la différence entre un objet quelconque et un objet connecté repose sur la connectivité de ce dernier. Pour connecter un objet à Internet, plusieurs choix s'offrent à vous. Vous en connaissiez déjà certains : le Wifi, le Bluetooth, le réseau cellulaire (3G, 4G). Ce sont des modes de connexion extrêmement répandus et grand public. Toutefois, certaines technologies comme le LPWAN ont été développées spécifiquement pour connecter les objets connectés. Elles ont pour but de minimiser la consommation énergétique, de maximiser la portée et de s'adapter au volume de données échangées.

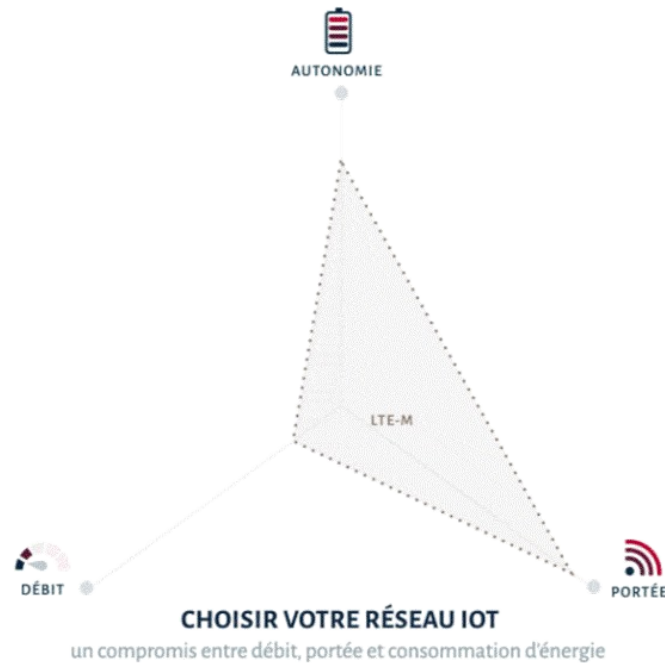
Pourquoi le choix du réseau IoT est-il déterminant ?

Vous savez déjà que l'usage de vos objets connectés dépend grandement de leur mode de connectivité. Prenons un exemple du quotidien, le son de votre enceinte Bluetooth coupe au-delà de quelques mètres, ou bien le Wifi de votre appartement est moins fiable dans la chambre à coucher que dans le salon. Pourquoi les enceintes de salon (type Sonos) sont-elles connectées en Wifi alors que les enceintes portatives sans fil le sont en Bluetooth, et non l'inverse ? Dans le premier cas, l'enceinte n'est faite que pour être utilisée de manière immobile, branchée sur secteur, dans une pièce où le réseau Wifi est disponible. Dans le second, l'enceinte Bluetooth peut être utilisée à la plage, recourant au réseau Internet de votre téléphone, par définition mobile.

Les 3 éléments fondamentaux d'un réseau IoT : Chaque réseau dispose de ses points forts et de ses points faibles. Cependant, chaque technologie peut être considérée en fonction de trois critères

- Sa **consommation d'énergie** (combien d'énergie consommée pour envoyer 1 Mo).
- Sa **bande passante** (combien de temps nécessaire pour envoyer 1 Mo).
- Sa **portée** (sur combien de mètres ou kilomètres la connexion reste fiable).

A ces critères s'ajoute la **fréquence** à laquelle vous devez récupérer les données captées par votre objet (en temps réel, une fois par heure ou par jour).



Prenons l'exemple d'une caméra embarquée dans une voiture, appelée dashcam. Nous avons besoin de récupérer le film enregistré uniquement en cas d'accident. Les dashcams connectées n'envoient donc le film à votre assureur qu'en cas de choc détecté, et suppriment les vidéos enregistrées au fur et à mesure le reste du temps.

Quel réseau IoT choisir pour connecter vos objets ?

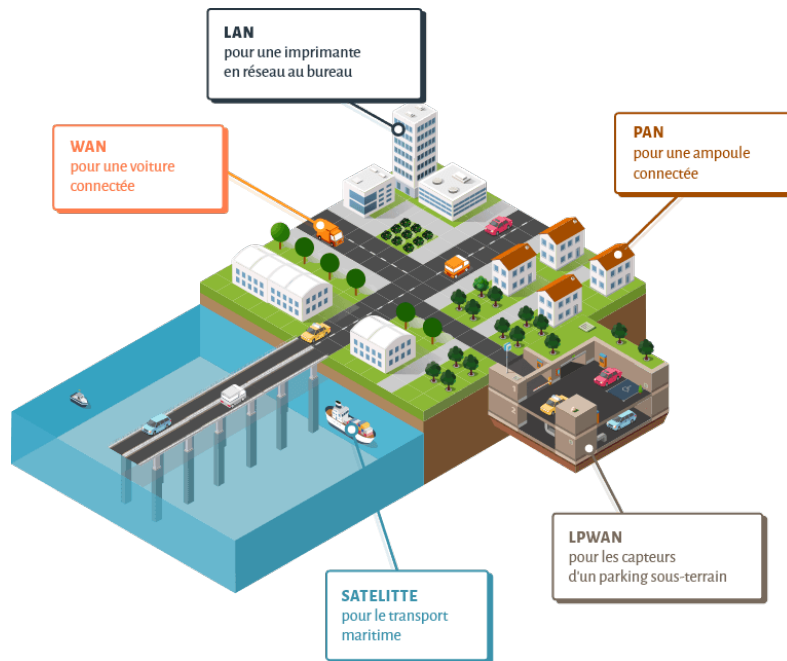
Passons en revue l'ensemble des technologies permettant à votre objet d'être connecté à Internet, en les classant en deux catégories :

1. Réseaux « **courte distance** » : de quelques centimètres à quelques mètres.
2. Réseaux « **longue distance** » : de quelques dizaines de mètres à plusieurs kilomètres.

Nous pouvons différencier les types de réseaux IoT selon cette typologie :

- **WAN** (Wide Area Network) : un réseau de plusieurs dizaines de kilomètres carrés
- **LPWAN** (Low Power Wide Area Network) : réseau de plusieurs dizaines de kilomètres carrés mais utilisant peu d'énergie (car peu de bande passante)
- **PAN** (Personal Area Network) : le réseau de quelques mètres (Bluetooth)
- **LAN** (Local Area Network) : le réseau Internet privé de votre domicile ou de votre entreprise (Wifi)

- **Satellite** : partout dans le monde pour peu de ne pas être dans un tunnel (GPS)



1. Les réseaux IoT *courte distance*

Bluetooth : Probablement la technologie la plus grand public, démocratisée depuis le début des années 2000. Sa consommation d'énergie est relativement faible ainsi que sa portée (environ **10 mètres**). Le Bluetooth possède une bande passante intermédiaire (**entre 1 et 3 Mb/s**) mais amplement suffisante pour la plupart des utilisations classiques. Le Bluetooth est un choix approprié pour beaucoup de **MedTech** (médecine). Par exemple, la société DiabNext permet de surveiller son diabète à l'aide de capteurs connectés au téléphone en Bluetooth.

Zigbee : Le Zigbee est un **protocole de communication** similaire au Bluetooth mais dédié à l'IoT. Il consomme peu, et est fait pour envoyer de petits volumes de données (**entre 20 et 250 Kb/s**). Il permet d'utiliser chaque objet comme "rallonge de connexion". Par exemple, l'ampoule connectée de votre salon va permettre de connecter l'ampoule de votre chambre, comme un relai jusqu'au "hub", branché au réseau Internet. Les objets connectés de Ikea ou Philips Hue utilisent Zigbee. Il s'agit d'envoyer en effet des ordres, tels que « **allumer la lumière** de la chambre », peu générateurs de données lourdes.

Wifi : Le Wifi permet un très important débit data (environ **400 Mb/s** pour les modems grand public récents), de manière fiable et sécurisée. Toutefois il consomme beaucoup d'énergie et sa portée est relativement limitée (**35 m**), d'autant plus au travers d'obstacles comme des murs épais. Le **Wifi 6**, aussi appelé Wifi AX, nouvelle génération en cours de commercialisation, va permettre d'améliorer considérablement la connectivité des objets connectés. Avec un débit de **10 Gb/s**, il permettra de gérer

beaucoup plus d'appareils plus efficacement tout en consommant moins d'énergie : il s'agit de limiter le mode veille des objets en les "réveillant" lorsqu'un échange de données est nécessaire. Le réseau Wifi très haut débit repose sur la couverture en fibre optique du territoire. Il est en effet nécessaire d'apporter le câble optique jusqu'à chaque terminal de chaque habitation ou entreprise. Si c'est le cas dans la plupart des villes, nous en sommes très loin dans les zones rurales. En plus des **opérateurs télécoms**, plusieurs entreprises réalisent des poses de fibre optique à la demande.

RFID : Un mode de connexion particulier, dédié à l'identification, on pourrait le surnommer code-barre 2.0. Une puce RFID permet d'identifier à distance, comme on le ferait en scannant un code-barre, mais jusqu'à **100 mètres**. C'est une technologie qui vient en complément d'autres types de connectivité. Aujourd'hui, la RFID est devenue une technologie indispensable pour gérer les ressources nécessaires au bon fonctionnement des chaînes de production industrielles. Néanmoins, si l'identification par radio fréquence permet de récolter l'ensemble des données sur le terrain, elle n'en permet pas la transmission. Pour pallier cela, la carte SIM M2M, via le réseau IoT cellulaire, prend le relai en rendant le transport des données possible. Voici deux exemples illustrés de synergie où la carte SIM M2M intervient en sur couche.

Allier RFID et carte SIM M2M pour exploiter les données

L'identification par radio fréquence via des badges, puces et tags RFID longue portée (plus de 100 mètres) est couramment mise en place pour la protection des biens (marquage antivol), pour la protection des ouvriers sur un chantier, pour effectuer des contrôles thermiques à distance et dans de nombreux autres secteurs. En effet, cette solution permet d'identifier et de localiser une personne ou un bien grâce à une puce embarquée.

Néanmoins, si ces puces permettent de récolter des données de localisation, d'identification et de contrôle en temps réel, la connectivité RFID ne permet pas de remonter l'information vers un site ou une plateforme et donc de la consulter à distance.

C'est là que la synergie entre en jeu : là où la puce RFID récolte les données, la carte SIM M2M permet leur transmission, et donc une gestion à distance et en temps réel des ressources. Certains chantiers utilisent en effet la RFID pour décompter les entrées et sorties des salariés intervenant sur site, notamment dans les tunnels, grâce à une puce intégrée au casque des travailleurs et un capteur placé à l'entrée du tunnel. Le décompte est alors consultable sur site, directement sur le compteur. La carte SIM M2M placée en sur couche prend le relais et permet la transmission des données vers une interface. De quoi faciliter des opérations comme la gestion, la maintenance, ou tout simplement fluidifier la diffusion des informations.

NFC (Near Field Communication) : Son utilisation la plus connue est le paiement sans contact. Le NFC peut échanger un **très petit volume** de données sur une distance très rapprochée (quelques centimètres). C'est une technologie largement répandue pour les ouvertures de portes dans les chambres d'hôtels.

Le WiFi direct, c'est quoi ?

Le WiFi direct n'est pas la même chose que le WiFi traditionnel. En effet, là où le WiFi n'est disponible que dans l'environnement immédiat d'un routeur (modem) sans fil, le WiFi direct désigne un protocole qui permet de connecter deux ou plusieurs appareils sans point d'accès intermédiaire (routeur ou modem).

Dans le cas d'une [connexion WiFi traditionnelle](#), si vous possédez un routeur ou une [box Internet](#), tous vos appareils informatiques qui y sont connectés peuvent dialoguer entre eux : échanges de fichiers, chat, etc. Le routeur (ou la box Internet) représente alors le cœur du réseau, toutes les informations échangées y transitent.

Quant au WiFi direct, c'est un protocole de transmission qui est comme son nom l'indique, direct et sans fil, entre 2 ou plusieurs appareils. Il existe depuis une dizaine d'années (Google a intégré le support logiciel du WiFi Direct dans le système Android à partir de la version 4.0 sortie en 2011). Les appareils se connectent directement entre eux sans avoir besoin de passer par un modem. C'est un peu le même principe que le [Bluetooth](#), qui lui existe depuis 1994, mais le WiFi direct est plus rapide (20 fois), efficace sur de plus grandes distances (100 mètres) et avec un débit plus performant. Le WiFi direct est une technologie qui a été créée par la WiFi Alliance, le consortium qui possède la marque «WiFi». Son objectif est de rassembler l'ensemble des acteurs du marché autour d'une même bannière pour assurer le développement technologique du WiFi, garantir l'interopérabilité des produits mais également promouvoir cette technologie sans fil. Sa promesse est de garantir que les équipements WiFi offrent la meilleure expérience utilisateur possible. Basée à Austin dans le Texas (USA), la WiFi Alliance possède un rayonnement mondial. Elle revendique plus de 800 membres en 2020. Parmi ses principaux sponsors, on retrouve entre autres Apple, Microsoft, Sony, LG ou encore Samsung. Le WiFi direct utilise un certain nombre de normes pour accomplir ses fonctions. Elles sont essentiellement les mêmes que celles de la technologie WiFi classique. Pour connecter deux appareils via le WiFi Direct, l'un d'entre eux crée un point d'accès similaire à celui d'un routeur. L'autre appareil le recherche et s'y connecte. Un des intérêts majeurs du WiFi direct est la possibilité de transférer des fichiers de n'importe quelle taille entre les deux appareils à grande vitesse.

[Comment fonctionne le WiFi direct ?](#) Concrètement, la procédure qui permet la création de la connexion WiFi direct entre deux appareils comprend deux «états» : l'écoute et la recherche.

- À l'état d'écoute, le périphérique attend de recevoir une requête de sonde à laquelle il peut répondre, appelée «analyse passive».
- L'état de recherche, ou «balayage actif», envoie des requêtes, en attendant les réponses des dispositifs dans un état d'écoute.

Pour créer le réseau P2P (modèle de réseau informatique d'égal à égal entre ordinateurs qui distribuent et reçoivent des données ou des fichiers), les deux périphériques doivent basculer activement entre les deux états.

Une fois que deux appareils se sont repérés l'un l'autre, ils entament des négociations sur l'appareil qui servira de propriétaire du groupe P2P (P2P GO). Le P2P GO permet à l'autre périphérique de s'y connecter.

Quelles sont les applications du WiFi direct ?

D'une manière générale, le WiFi direct sert à simplifier les démarches informatiques de votre quotidien. Une seule condition est requise : les deux appareils ainsi reliés doivent être certifiés WiFi direct pour échanger des données.

Le WiFi direct est potentiellement compatible avec les smartphones, les tablettes, les ordinateurs, les télévisions, les appareils photos, les imprimantes et bien d'autres périphériques. Aujourd'hui beaucoup de dispositifs et périphériques informatiques, tels que les lecteurs portables, les casques sans fil, les souris

d'ordinateur et les claviers, ou les imprimantes, utilisent le WiFi direct pour se connecter avec d'autres dispositifs au lieu de Bluetooth.

Précision : Tout appareil ou périphérique certifié WiFi direct est capable de communiquer avec les anciens équipements WiFi. Ainsi, si vous possédez un appareil photo numérique ayant la certification WiFi direct, il pourra communiquer directement avec votre imprimante WiFi classique.

Exemples d'applications du WiFi direct

Le WiFi direct peut vous permettre par exemple :

- D'envoyer des documents ou des photos d'un ordinateur à une imprimante, sans avoir besoin de renseigner une clé WiFi qui peut être parfois complexe.
- De transférer de données entre deux smartphones ou deux ordinateurs : en effet, certains media, comme par exemple une vidéo assez lourde, ne peuvent pas être transmis par email, car ils dépassent la limite autorisée par le serveur. En Bluetooth, cette démarche est parfois trop longue. Dans ce cas, et si le destinataire est à proximité, vous pouvez lui envoyer votre fichier via WiFi direct.
- De diffuser une vidéo d'un ordinateur ou smartphone sur une télévision : avec un téléviseur en WiFi direct, le transfert d'images est immédiat et quelques clics suffisent pour partager vos contenu audiovisuels : visionnez vos photos et vidéos prises avec votre smartphone sur grand écran, téléchargez des séries sur votre ordinateur ou votre mobile et regardez-les sur votre écran de télévision, réalisez instantanément des copies d'écran...

WiFi direct : comment établir une connexion entre deux appareils ?

Il existe plusieurs moyens d'établir la connexion WiFi direct : appuyer sur un bouton, rapprocher physiquement les appareils, entrer un code PIN ou un mot de passe, etc. Le WiFi direct reprend la sécurité du WiFi classique, et il est possible de sécuriser ses transferts avec une clé de sécurité comme sur un réseau classique.

WiFi direct Samsung et appareils Android

Le WiFi direct est disponible sur les appareils Android (à partir d'Android 4.0).

Pour l'utiliser, c'est très simple : Le WiFi direct se trouve dans les paramètres WiFi, à des emplacements légèrement différents selon les modèles. Vous devez l'activer sur les deux appareils qui devraient se détecter automatiquement après un balayage. Une fois que c'est le cas, établissez une connexion depuis l'un des smartphones en appuyant sur le nom du second. Ce dernier sera invité à confirmer la liaison.

À partir de là, vous pouvez transférer des fichiers de n'importe quelle taille entre les deux appareils très rapidement. Il vous suffit de sélectionner un fichier, d'appuyer sur l'icône de partage et de choisir «WiFi direct» dans la liste des options de partage. Sélectionnez ensuite l'appareil auquel le fichier doit être envoyé et le transfert se fait automatiquement.

précision : parfois, le partage ne fonctionne pas entre deux smartphones de différentes marques. Dans ce cas, vous pouvez avoir recours à une application tierce pour sauter cette barrière. Il en existe plusieurs comme par exemple Xender, SuperBeam ou encore SHAREit. Attention, il faut que l'application soit installée sur les deux appareils pour que cela fonctionne.

En plus de dispositifs Android avec WiFi direct, la norme peut aussi se trouver sur les consoles de jeux, telles que la nouvelle Xbox.

Le WiFi direct windows 10

La norme WiFi direct existe sur les appareils Windows, à partir de Windows 8.

Pour savoir si un PC Windows est compatible avec la norme WiFi direct, voici la marche à suivre :

1. Appuyez sur les touches Windows et R.
2. Saisissez «CMD» et appuyez sur la touche Entrée.
3. Saisissez «ipconfig /all | findstr Description».
4. Appuyez sur la touche Entrée.
5. Si Microsoft WiFi Direct Virtual Adapter s'affiche, votre PC Windows est compatible WiFi Direct.

Le WiFi direct sur les appareils iOS

D'un point de vue technique, les appareils Apple (iPhone, iPad et ordinateurs Mac) soutiennent le WiFi direct mais Apple a développé son propre système, via l'application AirDrop. Cela ne fonctionne alors qu'entre des appareils fonctionnant sous iOS.

Pour utiliser AirDrop :

1. Ouvrez une application, touchez «Partager» ou le bouton de partage. Si vous partagez une photo à partir de l'application «Photos», vous pouvez effectuer un balayage vers la gauche ou vers la droite et sélectionner plusieurs photos.
2. Sélectionnez l'utilisateur AirDrop avec qui vous souhaitez partager votre contenu (Si la personne avec qui vous partagez du contenu se trouve dans vos contacts, vous verrez une image avec son nom. Si elle ne figure pas dans vos contacts, vous verrez simplement son nom sans image). Vous pouvez également envoyer du contenu via AirDrop entre vos propres appareils Apple (par exemple d'un ordinateur à un iPhone ou inversement).

Le WiFi direct entre un téléviseur connecté et un ordinateur Windows :

Prenons l'exemple d'un téléviseur SONY compatible WiFi direct :

1. Activez le mode WiFi direct sur le téléviseur.
2. Appuyez ensuite sur Home (Accueil) sur votre télécommande, puis sur Applications et WiFi direct Mode (Mode WiFi direct).
3. Sur votre ordinateur, sélectionnez Control Panel (Panneau de configuration) dans le menu Start (Démarrer).
4. Sélectionnez Network and Internet (Réseau et Internet) (si cette option n'apparaît pas, sélectionnez Category (Catégorie) puis «View by» (Afficher par). Sélectionnez Connect to a network (Connexion à un réseau).
5. Sélectionnez DIRECT-xx-BRAVIA ou le SSID affiché sur le téléviseur.

6. Pour vérifier le SSID et les informations de clé WPA sur le téléviseur : appuyez sur OPTIONS sur votre télécommande et sélectionnez Manual (Manuel) puis Other Methods (Autres méthodes). Les informations de connexion (SSID et clé WPA) s'affichent.
7. Sélectionnez Connect (Connexion).
8. Saisissez la clé WPA affichée sur le téléviseur dans la fenêtre Security key (Clé de sécurité) et sélectionnez OK. Attention, la clé WPA étant sensible à la casse, veillez à la saisir exactement telle qu'elle apparaît sur le téléviseur, en respectant les minuscules et les majuscules.

Il peut arriver que le partage en WiFi direct ne fonctionne pas entre deux smartphones de marques différentes. Pour résoudre ce problème, il existe des applications comme Xender ou encore SuperBeam qui peuvent jouer ce rôle d'intermédiaire entre les deux appareils.

Le WiFi direct et la sécurité : quels sont les risques ?

Lorsque quelqu'un accède à un appareil via WiFi direct, il peut également être capable d'accéder à d'autres réseaux et à des données privées qui sont désormais ouvertes. Mais est-il possible de sécuriser une connexion en WiFi direct ?

Dans un premier temps, vous devez examiner la manière dont votre appareil sécurise votre connexion en WiFi direct et ce que vous pouvez faire pour la rendre plus sûre. Il y a deux types de connexions en WiFi direct : la connexion temporaire et la connexion permanente. La connexion permanente stocke les données sur les appareils pour qu'ils puissent à nouveau se connecter automatiquement, quand c'est nécessaire. Ces connexions permanentes sont un peu moins sûres et plus faciles d'accès, elles doivent donc être limitées à certains objets comme les imprimantes personnelles, et utilisées seulement quand c'est nécessaire. Les connexions temporaires quant à elles ne peuvent pas se rétablir toutes seules et ont besoin des étapes initiales : code PIN, identifiants etc. Cela les rend plus sûres.

Voici quelques conseils pour augmenter la sécurité de votre connexion :

- D'une manière générale, il est conseillé d'opter pour des connexions en WiFi direct récentes, car elles sont de plus en plus sécurisées.
- Il est déconseillé de vous connecter dans un endroit public, même si c'est avec un ami.
- Pensez à désactiver cette fonction de vos appareils lorsque vous ne l'utilisez pas. A titre d'exemple, même si ce n'est pas fréquent, il y a récemment eu un bug sur les appareils Linux qui a permis à des hackers d'accéder aux appareils lorsque le WiFi direct était activé. Il faut donc être vigilant car, de la même manière qu'un réseau WiFi classique, ce n'est pas infallible.

Fonctionnement des systèmes RFID et NFC. Les QR codes.

La communication en champ proche (ou Near Field Communication, ou NFC) est une technologie de communication sans contact de courte portée. La fonction NFC permet aux périphériques équipés de communiquer avec n'importe quel terminal mobile compatible en rapprochant simplement les deux supports ; aucune application n'est nécessaire sur l'un ou l'autre des téléphones.

Le NFC est un dérivé de la technologie RFID ; elle a commencé à être utilisée en France en 2011 mais reste encore peu courante. Toutefois, les smartphones sont maintenant de plus en plus équipés et les

initiatives se multiplient pour tester et développer l'utilisation de cette technologie. En France, son développement s'accélère grâce aux banques qui cherchent à démocratiser le paiement sans contact.

En résumé, le NFC c'est quoi ?

C'est une technologie mobile qui permet les interactions sans contact et qui équipe la plupart des smartphones.

Les différents modes de fonctionnement du NFC ?

Le NFC est une technologie sans contact qui permet de transmettre des informations digitales à un support mobile et qui fonctionne à proximité (environ 10 centimètres maximum) et à haute fréquence. Equipée sur un smartphone, elle peut-être utilisée selon différents modes :

Le mode émulation de carte

Dans le mode "passif" le terminal mobile se comporte comme une carte à puce sans-contact. Le téléphone envoie l'information au périphérique NFC, présent par exemple sur une borne de validation de titres de transport ou une borne de paiement. Les usages de ce type d'utilisation sont multiples: paiement, billets de spectacle ou transport, coupons, contrôle d'accès, etc.

Le mode lecteur

Dans le mode "actif", le mobile devient un lecteur de cartes sans contact. Ce mode permet de lire des informations en approchant son mobile d'un tag NFC. Les applications possibles sont également variées : tags NFC sur des affiches, pancartes, des monuments, arrêts de bus, ou encore sur des produits. L'objectif dans ce cas est de poursuivre une expérience sur son mobile en apportant un contenu digital. Dans ce mode, le tag NFC a un rôle comparable au **QR code** et peut être utilisé dans une campagne de **marketing Offline To Online**.

Le mode pair-à-pair

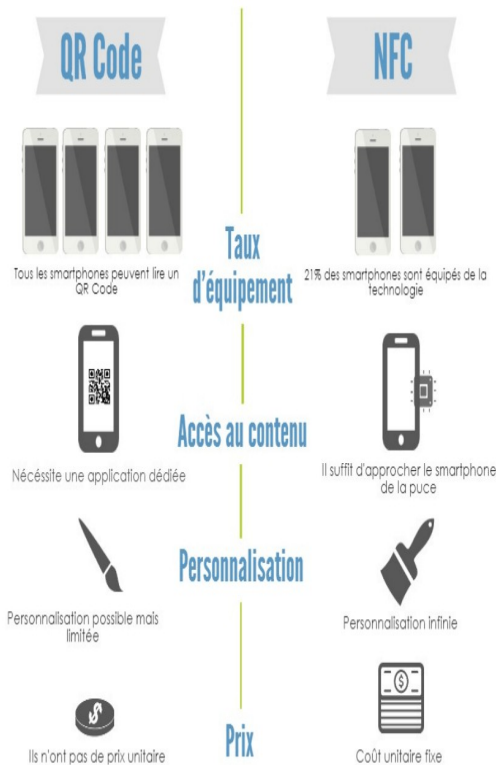
Ce mode fonctionne à double sens et permet à deux terminaux mobiles d'échanger des informations entre eux. Les applications peuvent être l'échange de cartes de visites (vCard), l'échange de fichiers (photos ou vidéos par exemple), de l'argent, etc.

NFC vs QR Codes

Le NFC et le QR Code sont deux technologies sans contact ayant la même fonction, mais qui sont pourtant très différentes.

Le taux d'équipement

Tous les smartphones peuvent potentiellement lire un QR Code, le téléchargement d'un lecteur de QR Code peut se faire gratuitement et en 3 clics. En revanche, seuls 22,4% des smartphones sont aujourd'hui équipés du NFC en France , ce qui représente tout de même un peu plus de 7 millions de terminaux mobiles.



L'accès au contenu

Pour lire un QR Code, l'utilisateur devra utiliser une application dédiée, un lecteur de QR Code. Pour lire un tag NFC, il suffira d'approcher son smartphone à moins de 10 cm de la puce NFC pour déclencher l'ouverture automatique du contenu sur le mobile.

La personnalisation

Aujourd'hui, les QR Codes peuvent être personnalisés aux couleurs d'une marque, et intégrer leur logo, mais il convient de respecter certaines règles pour qu'ils restent lisibles.

Les Tags NFC peuvent être personnalisés à l'infini ou même cachés dans le support de communication, leurs lectures n'en sera jamais affecté.

Le prix Les QR Codes n'ont pas de prix unitaire, ils peuvent être reproduits autant de fois que nécessaire, le tarif restera toujours le même. Les puces NFC étant un produit physique, chaque tag NFC intégré dans un support de communication a un coût.

NFC vs RFID

La Radio Identification, ou RFID (en anglais Radio Frequency Identification) est une technologie permettant d'identifier et caractériser un objet grâce à une étiquette émettant des ondes radio.

La RFID fait partie des technologies de localisation en temps réel (RTLS : Real Time Localisation System) et est utilisée principalement dans le cadre du traçage de marchandises dans de nombreux secteurs : retail, santé, transport et logistique, militaire et automobile.

Ainsi, le NFC est un dérivé de la technologie RFID mais présente quelques spécificités. La différence principale entre la RFID et le NFC réside dans le fait que la technologie NFC permet un transfert de données limité. Enfin, la technologie NFC fonctionne à très faible distance, quelques centimètres seulement contre plusieurs mètres pour la RFID.

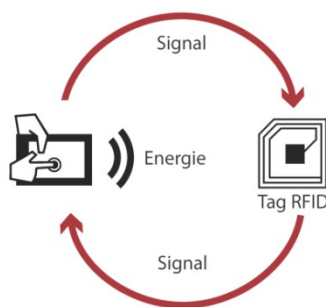
Comprendre la RFID : Avec le développement massif des produits RFID, il est important de bien comprendre comment la technologie fonctionne et comment l'utiliser de la manière la plus efficace. Comment fonctionne la technologie ? Quel est le support le plus efficace en fonction de l'utilisation qui en est faite ? Quelle puce choisir ? Pour vous repérer au mieux parmi le large choix de supports et de puces , voici quelques points simples auquel SBE répond :

La RFID qu'est ce que c'est ?

Tous les jours nous utilisons des produits RFID sans le savoir : à travers des cartes de transports, des étiquettes antivol dans les magasins, des badges RFID, badges de sécurité ou plus récemment des clés sans contact pour voiture.

Cette technologie a pour avantage de faire gagner du temps aux usagers et de permettre une lecture rapide des données. Mais qu'est ce que c'est vraiment RFID ?

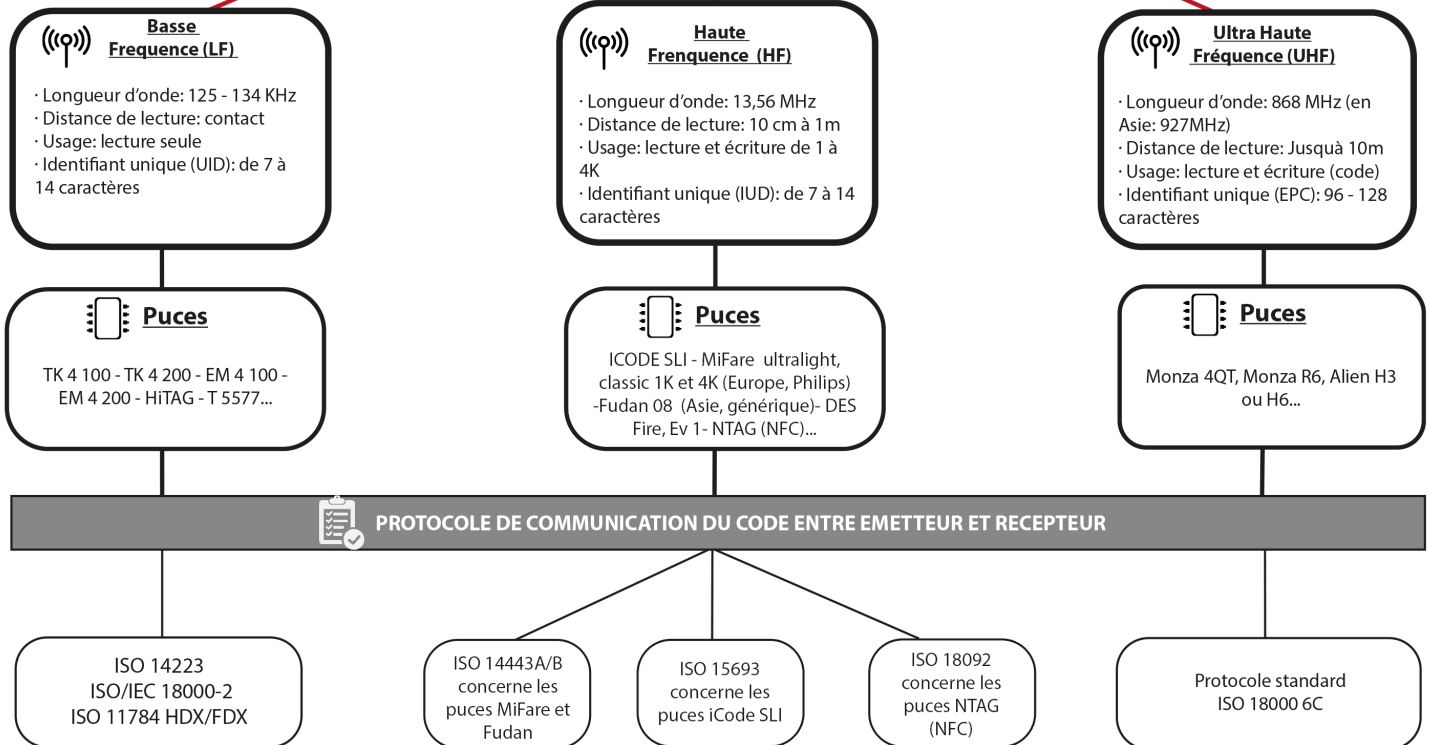
La RFID ou encore la Radio Frequency Identification est une méthode permettant de mémoriser et récupérer des données à distance. Le système est activé par un transfert d'énergie électromagnétique entre une étiquette radio et un émetteur RFID. L'étiquette radio composée d'une puce électronique et d'une antenne reçoit le signal radio émis par le lecteur lui aussi équipé d'une technologie RFID. Les composants permettent à la fois de lire et de répondre aux signaux.



Puce RFID ou puce NFC?



La RFID - qui est le diminutif de Radio Frequency Identification - est une technologie qui permet de lire rapidement des données afin de faire gagner du temps aux utilisateurs.
Ex: puces pour animaux domestiques, badges d'entrée, puces antivol, clés de voitures...



sbedirect.com

NFC signifie **Near-Field Communication** (communication en champ proche). Le NFC est également basé sur les protocoles RFID. La principale différence avec la RFID est qu'un dispositif NFC **peut agir non seulement comme un lecteur, mais aussi comme une étiquette** (mode d'émulation de carte). En mode "peer-to-peer", il est également possible de transférer des informations entre deux dispositifs NFC.

Les systèmes NFC fonctionnent sur la **même fréquence que les systèmes RFID HF** (13,56 MHz). Il n'y a donc que des limitations de portée de lecture à courte distance.

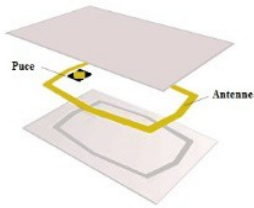
En raison de ces limitations, les appareils NFC doivent être **très proches les uns des autres**, généralement pas plus de quelques centimètres. C'est pourquoi la NFC est souvent utilisée pour les communications sécurisées, notamment pour les contrôles d'accès ou dans le secteur de la consommation pour le paiement sans contact.

Quel support pour les puces RFID et les puces NFC ?

Aujourd'hui, la RFID se développe sous différents supports :

Types de support

Objectifs



Cartes RFID et badges RFID

- Identification des personnes
- Paiement sans contact
- Contrôle d'accès en entreprise
- Transports Cartes de fidélité



Étiquette PVC sans contact RFID

- Identification & traçabilité
- 3 formats d'étiquettes RFID normes ISO
- Une technologie RFID performante et abordable
- 4 types de puces RFID disponibles



Étiquettes et stickers

- Identification des biens
- Stockage et inventaire
- Lutte contre la contrefaçon
- Traçabilité des produits
- Promotion dans les événements



Bracelets

- Identification des personnes
- Paiement sans contact
- Promotion dans les événements



Porte-clés et tags

- Accès à des résidences, locaux et parking
- Badge RFID d'accès en entreprise



Puces sous cutanés

- Identification d'animaux

Pour chacun de ces supports, la puce peut être à **usage unique (lecture seule)** ou bien **réinscriptible (lecture et écriture avec mémoire)**. Pour choisir le type puce, il faut tout d'abord choisir la fréquence en fonction de l'usage souhaité.

Quelles fréquences pour quelles distances de lecteur ?

La **fréquence est la caractéristique qui permet d'établir la communication** entre la puce et l'antenne. Toutes les puces sur le marché n'ont donc pas la même fonctionnalité.

Les puces se différencient en grande partie par la **fréquence de fonctionnement et la distance de lecture**. Plus la fréquence est élevée, plus la distance de lecture s'agrandit. En fonction de ces éléments, la puce sera plus ou moins puissante et plus onéreuse.

Trois types de fréquences sont utilisés pour les puces RFID :

- Basse fréquence (125Khz),
- Haute (13,56 Mhz)
- Très haute fréquence (UHF).

Types de fréquence	Fréquence de fonctionnement	Distance de lecture (m)	Taux de transfert	Normes
Basse fréquence	< 135 kHz	0.5	1kb/s	ISO 142231 ISO 18000-2
Haute fréquence	13,56 Mhz	1	25kb/s	ISO 14443 ISO 15693 ISO 18000-3
Très haute fréquence	863 à 915 Mhz	3 à 6	28kb/s	ISO 18000-6

Plusieurs fabricants se partagent le marché et proposent **des puces de plus en plus performantes**. Cette technologie est aujourd'hui standardisée et présente dans beaucoup d'objets du quotidien.

La puce RFID, active ou passive ?

Cette technologie se décline en trois versions :

- La RFID passive
- La RFID semi-passive
- La RFID active

La RFID passive fonctionne en lecture seule puisque la puce ne possède pas de batterie et doit être déplacé vers le lecteur pour être lu. Un puissant signal électromagnétique lui est alors envoyé, ce qui permet d'activer la puce RFID et de lire les informations qu'elle contient.

la RFID active fonctionne avec une source d'énergie telle qu'une petite pile ou une batterie, ce qui permet de lire la carte à plus longue distance. Cette technique est principalement utilisée pour la traçabilité de personnes, de véhicules ou encore pour la traçabilité logistique.

la RFID semi-passive est alimenté par une source d'énergie. Cependant, la batterie alimente la puce RFID à des intervalles de temps réguliers. Celle-ci n'envoie pas de signal. Cette technologie s'avère utile pour la traçabilité alimentaire notamment pour enregistrer les changements de température durant le transport.

Bien connaître les limites et les dangers RFID.

Pour pouvoir communiquer avec les étiquettes RFID, il faut un lecteur fixe ou portable. Ce lecteur a pour but de lire les données si elles ont été enregistrées à leur conception ou bien de modifier le contenu si la puce le permet.

Types	Caractéristiques	Distance de lecture	Fréquence
Fixe	Sous forme de portique ou bornes notamment en caisse de supermarché, en contrôle d'accès, à la bibliothèque.	Proximité : 25cm (le plus commun), Voisinage : jusqu'à 1m, Moyenne distance : jusqu'à 9m, Longue portée : centaines de mètres.	• Basse fréquence LF 125 Khz • Haute fréquence HF 13,56Mhz • Très haute fréquence UHF 868Mhz
Portable	Flasher portatif pour lire les étiquettes manuellement. Les étiquettes n'ont pas besoin d'être déplacé.	Quelques centimètres à quelques mètres	• Basse fréquence LF 125 Khz • Haute fréquence HF 13,56Mhz • Très haute fréquence UHF 868 Mh



Lecteur portable avec port RFID.



Lecteur-poignée fixe pour un contrôle d'accès.

La RFID au Quotidien.

Pendant des années, la RFID a été majoritairement présente dans la sécurité des personnes par le contrôle d'accès en entreprise ou dans la lutte contre le vol en magasin.

Aujourd'hui, elle a pour principale mission d'identifier :

- Des objets contre le vol, dans la gestion des stocks...
- Des personnes grâce aux cartes sans contact, aux passeports...
- Des animaux domestiques, sous forme de puces électronique sous-cutanée

On retrouve aussi la RFID dans l'information et la publicité dans certaines villes comme à Tokyo où 10 000 Marqueurs RFID ont été installés dans les rues afin d'informer les piétons lors de leurs déplacements ou encore pour envoyer certaines promotions dans la rue. Paris a, quant à elle, inséré des puces RFID dans 95 000 arbres pour assurer un suivi.

Amélioration du quotidien



Pour simplifier la vie des ménages, **les entreprises ont introduits la RFID dans beaucoup d'objets du quotidien** tels que les péages électroniques d'autoroute, les transports en commun (pass Navigo), les passeports biométriques, le paiement sans contact.

Dans le futur, nous pourrions voir la RFID dans d'autres domaines tels que **la médecine, dans les poubelles publiques, ou reliés à une connexion Wi-Fi**. Esso a, par exemple, mis en place un système qui permettrait de s'approvisionner en carburant grâce à un lecteur positionné dans sa voiture.

Lutte contre la contrefaçon

La RFID permet également de **lutter contre le vol à l'étalage** grâce à des étiquettes antivol discrètes à poser directement sur le produit ou sur l'emballage.

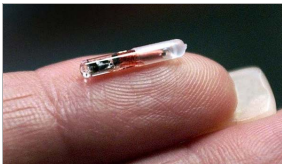
La RFID : une amélioration de la performance en entreprise.

De nombreux distributeurs et entreprises de logistique trouvent de nouvelles utilités à cette technologie : **la gestion des bagages en aéroport, l'inventaire en boutique, le picking en rayon ou la gestion des stocks** dans sa globalité.



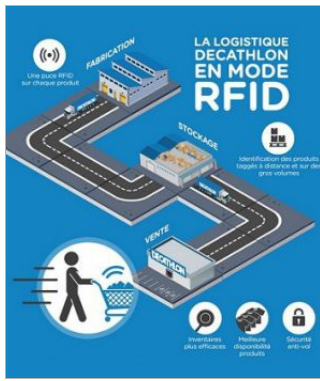
La traçabilité des produits

Il est possible de suivre un produit portant une étiquette RFID de **sa fabrication jusqu'à sa vente en caisse**. L'analyse de ses données permet d'**optimiser la chaîne logistique, de gagner du temps et de l'argent**.



L'une des utilisations les plus anciennes pour ce type de procédé vient des **années 80 pour l'identification et la traçabilité du bétail**. La technologie RFID permet de contrôler les animaux de leur naissance jusqu'à l'abattage sans fraude, pour **une meilleure traçabilité pour le consommateur et l'agriculteur**.

Aujourd'hui, de plus en plus de **puces sous cutanées** sont introduit sous la peau de certains animaux notamment pour une meilleure identification des animaux de compagnie (en cas de perte) ou un contrôle des animaux en voie de disparition.



Dans l'industrie, **cette étiquette est posée sur le produit ou sur son emballage au cours de sa fabrication**. La puce permet de tracer le produit durant son parcours : pendant le transport, le stockage ou encore la mise en rayon dans un magasin. Cette technique permet d'**estimer au mieux le coût et la durée de la chaîne logistique**. Aussi, cela permet d'anticiper des dysfonctionnements et d'obtenir un historique du produit en cas de dommages.

La gestion des stocks



Dans les magasins et usines qui possèdent des stocks, le tag RFID est le moyen d'**analyser rapidement les flux**. Le système informatisé permet d'avoir **une trace des flux : du stock jusqu'à la vente**. La caisse communique avec l'ordinateur mettant ainsi à jour la liste du stock.



Cette technique permet de maîtriser au mieux **le coût de ses stocks**. La technologie informe de l'arrivée et de la sortie du produit. En cas de vol dans un stock, il est possible de retracer le parcours du produit. Au-delà des stocks, les magasins peuvent également **accélérer l'inventaire en boutique**. Des entreprises telles que Tesco, une marque britannique, utilisent des robots équipés de lecteurs RFID pour lire les puces et faire l'inventaire.



Les étiquettes RFID permettent de **reconnaître un produit et d'obtenir toutes ses caractéristiques**. Ce procédé s'est notamment vu sur des étiquettes authentifiant du vin dans le but d'éviter le vol et la contrefaçon. Pour optimiser au mieux sa chaîne logistique, des entreprises comme Décathlon utilisent la technologie RFID pour **reconnaître les produits et les échanger sans tickets de caisse**.

Les limites du RFID : Comme toute technologie, la RFID possède ses propres limites. La diffusion de l'information pose problème pour toutes les questions sur **la sécurité de la vie privée**. Une carte non sécurisée peut être facilement **copiable pour récupérer ou modifier les données sensibles**.



De ce fait, il est nécessaire d'apporter plus de sécurité, pour cela il faut :

- **Protéger les cartes** et badges RFID d'accès grâce à des **étuis de protection** empêchant la récupération des données,
- **Limiter la durée de vie des données** enregistrées sur les cartes RFID (La carte Navigo ne donne que les trois dernières stations pour ne pas tracer les individus et éviter la fraude),
- **Chiffrer ou coder les données** pour ne pas risquer de divulguer des informations sensibles telles que des informations d'identités, des données bancaires...
- Pour permettre l'identification d'une carte, **associer une photo** pour reconnaître le propriétaire de la carte ou imprimer un hologramme pour authentifier la carte.

Aussi, toutes les puces ne sont pas lisibles à la même distance et dans les mêmes conditions. **La transmission des ondes est limitée à travers certains murs et certains métaux**. Certains métaux peuvent par exemple protéger la puce RFID de toute fraude.

Cette technologie a encore de beaux jours devant elle. Les possibilités d'utilisation sont immenses quel que soit le domaine d'activités des entreprises. Les puces peuvent être encodées par des **imprimantes RFID** ou **lecteurs RFID** pour modifier les informations (identifiants, données sensibles...).