

# Machine To Machine (M2M) Définition, Services et Adressage

EFORT

<http://www.efort.com>

Les communications entre machines ouvrent un formidable champ d'innovation. Quoique récentes, les technologies Machine To Machine (ou M2M) sont aujourd'hui suffisamment éprouvées pour qu'un très grand nombre d'entreprises puissent, en confiance, engager leurs propres projets : innovation dans les services et les usages, optimisation des processus-métiers, etc. Le Machine To Machine devient ainsi, dès aujourd'hui, un facteur majeur de compétitivité pour les acteurs économiques.

Le M2M résulte de la convergence de trois familles de technologies : des objets intelligents reliés par des réseaux de communication avec un centre informatique capable de prendre des décisions.

Les usages du Machine To Machine sont multiples : La gestion de flotte, la gestion de la chaîne d'approvisionnement (Supply Chain Management), la télésurveillance, la surveillance des biens et des personnes, la domotique résidentielle ou d'entreprise, le télépaiement automatique.

Le but de ce tutoriel est de définir précisément ce qu'est le M2M, de présenter des domaines d'application M2M et de montrer les solutions d'adressage des devices M2M. Un prochain tutoriel traitera des solutions d'optimisation du réseau mobile afin de supporter un très grand nombre de devices M2M.

## 1 M2M : Une définition

M2M consiste en l'utilisation d'un device (e.g., capteur, compteur, etc) pour capturer un événement (e.g., température, mesure sismique, consommation d'électricité, qualité de l'eau état d'environnement, etc.) qui est relayé à travers un réseau de communication mobile, fixe ou hybride à une application (e.g., du système d'information de l'entreprise qui utilise ces devices M2M). Cette dernière traduit l'événement capturé en des informations significatives (un inconnu a pénétré le local sans autorisation, la température a dépassé le seuil acceptable, la qualité de l'eau n'est pas satisfaisante, etc).

Une solution M2M est le résultat d'une interaction continue entre les devices M2M, les réseaux de communication et les applications.

Un device et une application co-localisés n'ont pas de relation M2M.

M2M doit être considéré comme le diminutif de M2(CN2)M qui signifie Machine-to-Communication Network-to-Machine. Il est aussi appelé Machine Type Communication (MTC) dans les recommandations 3GPP.

## 2 Architecture M2M

Comme indiqué à la figure 1, le M2M permet un échange bidirectionnel d'informations entre le device M2M et l'application. L'information reçue est ensuite traitée.

Dans de nombreux cas, le M2M implique un groupe de « devices » semblables interagissant avec une application.

Dans certains cas, les devices dans le groupe ne peuvent pas directement communiquer avec l'application du fait de leurs capacités limitées. Dans ces conditions, un équipement de médiation (GW, Gateway) est nécessaire, permettant de consolider la communication

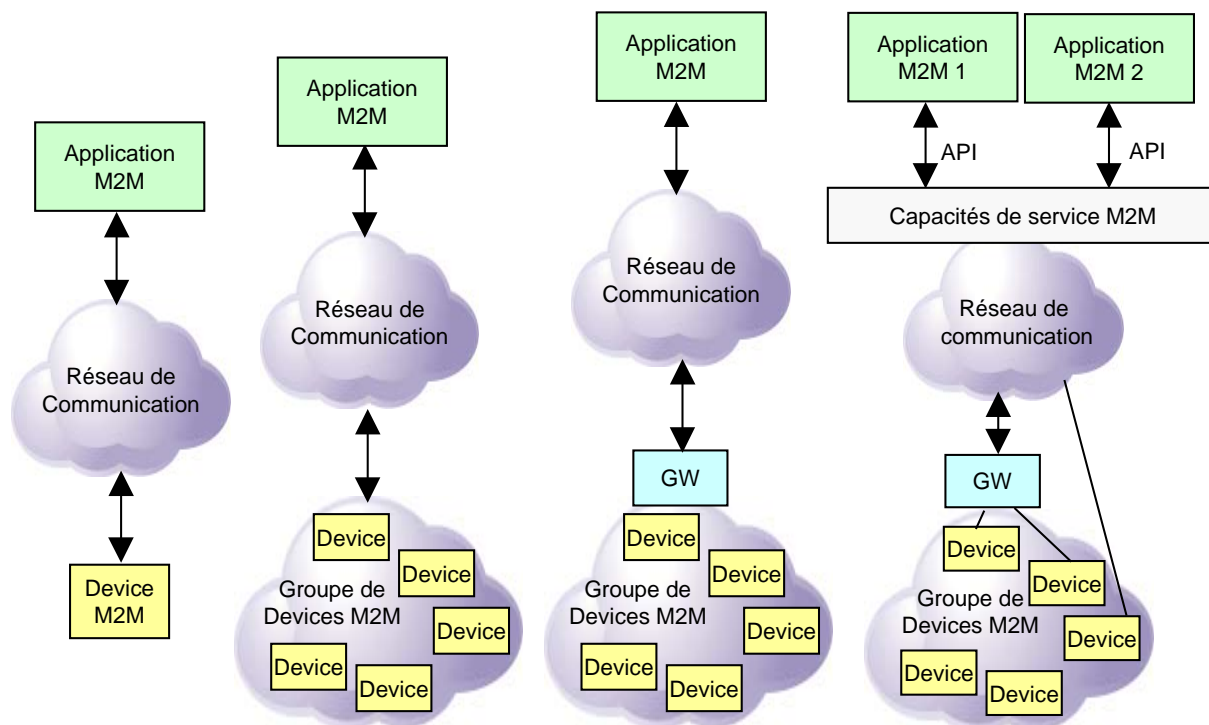


Figure 1 : Architecture M2M

Une plate-forme de services M2M (capacités de service M2M) peut être intégrée dans l'architecture M2M. Elle est mise en oeuvre par un opérateur M2M. Elle représente un middleware entre les applications se trouvant dans les systèmes d'information des entreprises clients de l'opérateur et le réseau de communication. La plate-forme de service M2M :

- Fournit des fonctions M2M2 utilisables par différentes applications
- Expose des fonctions via un ensemble d'interfaces ouvertes
- Utilise les fonctionnalité du réseau cœur
- Simplifie et optimise le développement et le déploiement d'applications en cachant les spécificités réseau

### 3 Quel réseau de communication pour le M2M ?

En théorie les réseaux de télécommunication fixe et mobiles sont utilisables dans le contexte du M2M.

Pour un grand nombre de devices M2M, (e.g., suivi de flottes de véhicules), l'unique option est un réseau mobile.

Pour les devices M2M qui sont stationnaires et qui pourraient s'accommoder d'une connectivité via un réseau fixe (e.g., compteur électrique), le monde mobile est tout de même préférable car :

- Le device M2M peut se trouver dans une aire difficile d'accès où la connectivité via le réseau fixe aurait un prix élevé.
- Si l'opérateur de réseau M2M dispose d'accords de roaming avec les opérateurs mobiles du pays concerné, le device M2M peut se rattacher à n'importe quel opérateur mobile en fonction de la qualité des signaux reçus. Cette flexibilité permet une meilleure disponibilité de la connectivité.
- Si les usagers finaux disposent déjà d'une connectivité avec différents opérateurs fixes, la compagnie d'électricité aura peut-être à adapter le device M2M en fonction des

différents opérateurs fixes impliqués. Si l'utilisateur oublie de payer sa facture, la ligne fixe pourra être coupée, ce qui empêchera la compagnie d'électricité d'obtenir les rapports du device M2M.

## 4 Opérations principales M2M

Dans toute solution M2M, il y a quatre opérations principales: la récolte de données, son transport et son traitement et le réveil du device afin qu'il puisse émettre un rapport de données non programmé.

Récolte de données (domaine de l'électronique) : La remontée d'informations se fait grâce aux capteurs embarqués dans les devices M2M. Les évolutions technologiques dans ce domaine donnent naissance à des dispositifs de moindre taille, moins coûteux et moins consommateurs en énergie.

Transport des données (domaine des télécommunications) : Plusieurs technologies de réseaux, radio ou filaire, peuvent coexister dans une même solution M2M. Le choix technologique dépendra de la couverture requise, du mode de connectivité, de la quantité de données à transmettre, de sa fréquence et du modèle économique.

Traitement des données (domaine de l'informatique) : L'application reçoit les données, les traite et intègre les données résultantes dans le système d'information de l'entreprise.

Réveil pour envoi de données (domaine des télécommunications) : Les devices M2M sont généralement programmés pour se réveiller à intervalle de temps fixe (e.g., toutes les heures), réaliser des mesures, s'attacher au réseau, établir une connexion de données, transférer leur rapport, puis libérer leur connexion et se détacher du réseau. Il peut arriver que l'application souhaite que le device M2M lui communique un rapport de données non programmé. L'application réveille donc le device par exemple par SMS et ce dernier transmet les données au serveur M2M.

## 5 Les domaines d'application du M2M

### 5.1 L'automobile

Le marché automobile présente un potentiel énorme avec 2 millions de véhicules immatriculés par an en France.

On peut identifier trois leviers qui encouragent les constructeurs à intégrer la connexion des véhicules dans leur stratégie et leurs chaînes logistiques :

- Améliorer la sécurité. Le projet européen e-call prévoit notamment que toutes les voitures neuves soient équipées d'une carte SIM à partir de 2015 afin d'intégrer un appel d'urgence automatique dans chaque véhicule. Lorsqu'un accident a lieu, d'après les différents capteurs présents dans le véhicule, ce dernier qui dispose d'un device M2M réalise un appel d'urgence (112 partout en Europe). Le centre d'urgence reçoit donc un appel dont le message d'établissement d'appel peut contenir certaines informations concernant les dommages causés par l'accident. Le centre d'appel peut aussi rappeler le numéro associé à la carte SIM du véhicule pour rentrer en communication avec l'automobiliste. Ce même module M2M peut être utilisé pour la lutte contre le vol par géolocalisation du véhicule, et pour le diagnostic des problèmes techniques (envoi de données au constructeur sur les problèmes techniques rencontrés par le véhicule).
- Permettre la gestion de sa flotte de véhicule (Fleet Management). Le secteur du transport est aujourd'hui le premier consommateur de données M2M. Les applications permettent de suivre les véhicules en temps réel et ainsi d'optimiser les tournées de livraison ou de savoir quel véhicule est le plus proche d'un point d'intervention.

- Offrir des services « infotainment » à valeur ajoutée comme axe de différenciation et d'innovation. L'objectif des constructeurs automobiles est bien de donner la possibilité aux conducteurs et passagers de bénéficier d'une galaxie de services cohérente avec un usage en mobilité.

## 5.2 L'énergie et la télémétrie

L'objectif de la télémétrie est de contrôler à distance des biens ou des personnes. C'est le cas dans l'énergie avec les compteurs dits intelligents.

La télémétrie dans le secteur de l'énergie assure à la fois la télémaintenance, la prévention et le relevé d'informations.

Il s'agit de récupérer les données des compteurs pour mesurer la consommation, faciliter et fiabiliser la facturation, étudier les tendances de consommation, et anticiper d'éventuels pics de consommation.

La lecture automatique à distance des compteurs permet de réduire considérablement les coûts (par rapport à une lecture manuelle). Le fournisseur pourrait par ailleurs envisager de mettre l'information à disposition de l'utilisateur, lui permettant ainsi une meilleure gestion de sa consommation.

## 5.3 Distributeurs automatiques de biens consommables

Connecté par réseau filaire ou GSM à un serveur, le distributeur signale son état. Par exemple, il indique que ses réserves sont épuisées et automatiquement, le livreur reçoit l'information pour aller approvisionner ce distributeur. Les bénéfices sont :

La maîtrise du parc : Remontée en temps réel des informations du distributeur : les ventes par produit, l'état des stocks, les revenus dans la machine. Les données sont accessibles dans une application web sous forme de tableaux de bord par exemple.

Diminution des interventions sur les sites grâce à la remontée de dysfonctionnements en temps réel

Diminution du taux d'indisponibilité des distributeurs par intervention immédiate suite à dysfonctionnement

Optimisation du réapprovisionnement par connaissance de l'état des stocks dans le distributeur

## 5.4 La santé et le suivi à distance des patients

Le recours à des processus automatisés supervisés par une plateforme M2M pour collecter les informations des patients pourrait permettre de décharger les hôpitaux du suivi de certains patients et de leur offrir la possibilité d'être hospitalisés à domicile plutôt que d'occuper une chambre d'hôpital. Cela pourrait aussi réduire le nombre d'interventions des soignants à domicile tout en optimisant la collecte de données. Les ressources libérées grâce à ces optimisations pourraient permettre de consacrer plus d'efforts et de ressources au problème chronique de la congestion des centres d'urgences.

Cette solution est destinée à prendre en charge à distance des patients ayant une pathologie (e.g., diabétique, souffrant d'hypertension, etc).

Les données (e.g., rythme cardiaque, la tension artérielle, le poids ou l'oxygénation du sang, le taux de glycémie), lues quotidiennement par les capteurs d'un équipement spécifique chez le patient, sont transmises automatiquement via un téléphone mobile ou un Gateway relié au réseau mobile à un centre de gestion accessible aux médecins par Internet.

Ces derniers renvoient un avis médical au patient par SMS ou par message vocal.

Les consultations sont anticipées. Le patient et le médecin sont informés à temps de toute complication éventuelle.

## 5.5 La domotique

La domotique est l'ensemble des techniques de l'électronique, de physique du bâtiment, d'automatisme, de l'informatique et des télécommunications utilisées dans les bâtiments et permettant de centraliser le contrôle des différentes applications de la maison (système de chauffage, volets roulants, porte de garage, portail d'entrée, prises électriques, etc.).

La domotique vise à apporter des fonctions de confort (gestion d'énergie, optimisation de l'éclairage et du chauffage), de sécurité (alarme) et de communication (commandes à distance, signaux visuels ou sonores, etc.) que l'on peut retrouver dans les maisons, les hôtels, les lieux publics, etc.

## 5.6 La surveillance et la sécurité

Les devices de surveillance et de sécurité sont principalement déployés dans des aires résidentielles ou dans les locaux de petites entreprises afin de fournir des informations de surveillance via des vidéos ou des photos à des application de gestion d'alarmes de sécurité ou aux propriétaires de ces locaux.

Les informations échangées sont principalement composées d'information d'alarmes et de manière occasionnelle de données multimédia (vidéo et photo) avec une résolution faible ou moyenne.

# 6 Echange de données entre le device et le serveur M2M

Deux procédures sont à prendre en compte pour la communication entre le device et le serveur M2M : le transfert de données et le déclenchement ou réveil du device.

Pour les devices MTC qui transmettent de très petits volumes de données, l'utilisation des services du domaine circuit, tels que le SMS semble plus efficace globalement.

Pour un déploiement donné, les choix technologiques peuvent être :

Pour l'échange des données :

- Services du domaine circuit (CS) tels que SMS et circuit switched data (CSD). L'utilisation du domaine CS concerne les applications M2M qui transmettent de très petits volumes de données de façon occasionnelle. Le CSD offre des débits très faibles (9,6 kilobits/s, parfois 14,4 ou 28,8 ou 43,2 kilobits/s en HSCSD (High Speed Circuit Switched Data). Avant que n'apparaisse GPRS, CSD a été déployé comme technologie pour les applications M2M. CSD est la forme initiale de transmission de donnée, développée par les systèmes GSM. Elle permet un débit de 9,6 kbit/s montant et descendant, ce qui semble suffisant pour les premières applications M2M (émission de mesures, informations d'état, etc.) . La tarification du service CSD est fonction de la durée de la connexion CSD.
- Services du domaine paquet (PS) tel que le contexte PDP (2G/3G) ou le bearer (4G). Aujourd'hui la majorité des devices M2M sont des devices 2G même si il commence à apparaître un usage 3G. L'utilisation du domaine PS concerne les applications M2M qui transmettent des volumes de données moyens ou importants ou qui requièrent une latence courte. Un contexte PDP peut être établi de façon permanente (always-on) ou à l'initiative du device M2M lorsqu'il le nécessite.

Le déclenchement de device (device triggering) concerne les mécanismes utilisés par un serveur M2M pour déclencher l'établissement d'un contexte PDP par un device M2M pour le transfert du rapport de données généré.

Alors qu'il est souhaité que chaque device ait une connectivité data always-on et une adresse IP assignée de manière permanente, ce type de configuration est coûteux en terme d'usage de ressources réseau et de consommation d'énergie.

Les solutions de déclenchement du device M2M par le serveur M2M sont:

- Envoi d'un SMS spécifique au device M2M : Le device est attaché au réseau circuit mais pas au réseau paquet. Ainsi il peut recevoir le SMS. Le device réagit alors en produisant son rapport, et le transmet en se rattachant au réseau paquet et en établissant un contexte PDP (procédure PDP context activation).
- Initiation d'un appel voix sans réponse : le serveur M2M déclenche l'établissement d'un appel voix à destination du device M2M. Ce dernier reconnaît le numéro d'appelant mais ne répond pas à l'appel (ainsi l'entreprise ne paie pas le déclenchement à la différence de la solution basée sur le SMS). A la suite, le device produit son rapport, s'attache au réseau paquet, établit un contexte PDP/bearer et transmet le rapport.
- Etablissement d'un contexte PDP initié par le réseau (network initiated PDP context activation) : Cela permet au réseau pour le compte du serveur M2M d'initier l'établissement du contexte PDP. Cette fonctionnalité permet d'éviter l'envoi d'un SMS ou l'établissement d'un appel, mais n'est quasi jamais supportée dans les réseaux GPRS opérationnels.
- Contexte PDP permanent : Le device M2M est toujours attaché au réseau paquet et dispose d'un contexte PDP permanent. Le serveur M2M peut alors envoyer la demande de déclenchement de device directement sous forme d'un message sur IP qui est reçu par le device M2M via le contexte PDP. Le device M2M peut alors envoyer son rapport sur ce même contexte PDP.

Le déclenchement du device n'a pas pour seul objectif le réveil du device afin qu'il émette un rapport au serveur M2M. Dans le cas où le device ne dispose pas de contexte PDP permanent, le déclenchement est nécessaire afin que le device établisse le contexte PDP et permette ainsi au serveur d'émettre des données au device (e.g., mettre à jour des logiciels sur le device M2M, mettre à jour des paramètres de configuration sur le device, etc.).

## 7 Adressage des devices M2M

Le device MTC avec sa carte SIM dispose de l'IMSI. Cet identifiant lui permet de s'identifier au moment de l'attachement au réseau mobile et de s'authentifier. L'IMSI est par définition une identité privée et non publique.

Mais le device ouvre un contexte PDP / bearer et obtient une adresse IP (IPv4 ou IPv6). Est-ce suffisant?

Il est nécessaire de produire les informations de taxation pour les services utilisés par le device MTC. Généralement le MSISDN associé à la souscription MTC est l'identité utilisée par les applications de facturation.

Il est nécessaire de réveiller le device alors que le device ne dispose pas de connectivité always-on. Le réveil peut alors être réalisé via SMS utilisant le MSISDN. Le serveur MTC utilise dans ce cas l'identité publique du device MTC.

Même si le device M2M dispose d'une connectivité always-on, il est possible que le serveur MTC veuille demander un rapport au device. Dans ce cas, il est nécessaire que le serveur connaisse l'adresse IP du device pour le réveiller, ce qui n'est pas toujours le cas, si le device n'a jamais encore interagit avec le serveur. Un hostname de device MTC connu par le serveur MTC pourrait alors être traduit via le DNS en adresse IP.

Tout nouvel adressage public doit pouvoir fonctionner même en situation de roaming.

### 7.1 MSISDN à 10 chiffres

En France, les numéros mobiles ont un des formats suivants : 06 XX XX XX XX et 07 XX XX XX XX. Ce plan de numérotation permet un maximum de 200 millions de souscriptions, suffisant pour 65 millions d'habitants mais vite limité pour le M2M si à terme, il est déployé massivement. Une alternative aurait été l'utilisation de MSISDN privés mais ne permettrait

pas le roaming des devices M2M (tels que des flottes de véhicules connectés traversant la frontières).

## 7.2 MSISDN plus long

Une alternative à la solution actuelle est donc l'extension de la longueur du MSISDN à 12, 13, 14 ou 15 digits. La taille maximum d'un MSISDN est 15 digits et consiste en un Country Code (CC), un National Destination Code (NDC) et un Subscriber Number (SN). Alors que la longueur des nombres CC et NDC peut être différente selon les pays, la majorité des nombres SNs ont une taille d'environ 10 digits. Cela permet d'adresser 10 milliards de terminaux différents.

Cette alternative d'extension de la taille du MSISDN est attractive dans certaines régions. Dans d'autres comme les Etats-Unis, le schéma de réseau et de commutation est conçu sur un MSISDN sur 10 digits et le coût d'extension à 12 digits ou plus, dépasserait les 100 milliards de dollars.

En France, l'ARCEP a ouvert une tranche de numéros mobiles de longueur étendue à 14 chiffres commençant par 0700 qui a vocation à être notamment utilisée pour les communications M2M. La création de tranches de numéros de longueur étendue à 14 chiffres ouvre une ressource de 10 milliards de numéros par ouverture de tranche « ZAB », qui réduit ainsi le risque de pénurie.

## 7.3 Uniform Resource Indicator

L'autre option est d'utiliser un Uniform Resource Identifier (URI). L'URI peut être converti en adresse IP grâce au DNS. Il s'agit d'un concept bien connu dans le monde Internet

Le format possible d'URI est : `issi:deviceId.userId.serviceproviderid.topdomain`

où issi = International Service provider Subscription Identifier

Par contre, utiliser l'URI implique mettre à jour les nœuds du réseau qui fonctionnent aujourd'hui avec le MSISDN tels que les HLR/HSS, les SGSN, les SMSCs, etc. Par ailleurs, les applications de facturation qui traitent la CDRs à partir du MSISDN devront être adaptées pour utiliser l'URI.

## Références

« M2M Communications : a Systems Approach », édité par David Boswarthick, Omar Elloumi, Olivier Hersent.