Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

30-Jan-2012

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

Working Party on Communication Infrastructures and Services Policy

MACHINE-TO-MACHINE COMMUNICATIONS: CONNECTING BILLIONS OF DEVICES

JT03315036

DSTI/ICCP/CISP(2011)4/FINAL
Unclassified

English - Or. English

FOREWORD

This report was presented to the Working Party on Communication, Infrastructures and Services Policy (CISP) in June 2011. It was recommended to be made public by the Committee for Information, Computer and Communications Policy (ICCP) in October 2011. The report was prepared by Mr. Rudolf van der Berg. It is published under the responsibility of the Secretary-General of the OECD.

TABLE OF CONTENTS

Boxes

MAIN POINTS

This document examines the future of Machine-to-Machine communication (M2M), with a particular focus on mobile wireless networks. M2M devices are defined, in this paper, as those that are actively communicating using wired and wireless networks, are not computers in the traditional sense and are using the Internet in some form or another. While, at the global level, there are currently around five billion devices, connected to mobile networks, this may by some estimates increase to 50 billion by the end of the decade. The report provides examples of some of the uses to which M2M is being put today and its potential to enhance economic and social development.

This report concludes that to achieve these benefits, however, changes to telecommunication policy and regulatory frameworks may be required. Some of the main areas that will need to be evaluated, and implications of M2M assessed, include: opening access to mobile wholesale markets for firms not providing public telecommunication services; numbering policy; frequency policy; privacy and security; and access to public sector information.

Use of M2M is shifting the market from one where users have a relatively limited number of communication devices to thousands or, in the case of business users, potentially millions of devices. Business users have tremendous flexibility with the Internet, directly offering or outsourcing to meet their needs but, due to regulation, are more limited in respect to their choices for mobile wireless M2M services. Moreover, the national focus of some regulatory settings, or the commercial service areas of infrastructure providers and consequently their service offerings, may combine to act as a significant barrier to the efficient use of M2M services across borders.

Further liberalisation, in wireless markets, could enable M2M-users to buy wholesale access to mobile networks, to change mobile networks without switching SIM-cards and to directly negotiate national and international roaming. This would, however, involve changes to current numbering policies regarding IMSI-numbers for SIM-cards and telephone numbers, so that not only traditional telecommunication companies, but also M2M-users could access these numbers. Such changes could lead to a more dynamic market for mobile wholesale access, mobile roaming and a strengthening of competition between mobile network operators.

A further area, for the future of M2M, is that numbering policy in this respect will need to be considered. Some countries, in the OECD area, are set to fully utilise the stock of telephone numbers under their current numbering plans. This does not mean that they do not have any numbers available, but rather that the current ranges for mobile communication may be insufficient for future requirements. There are different options to address this issue and they will need to be considered by relevant authorities.

M2M will make extensive use of wireless communication in both licensed and unlicensed spectrum bands. For licensed spectrum, policy makers will need to take into account that M2M has a much longer expected life than traditional wireless communication - up to 30 years instead of five to seven years. For example, the current use of 2G mobile wireless for M2M may mean that mobile networks will not be able to shut down their 2G networks, even if they wish to, because a countries smart metering infrastructure depends on 2G. This could rigidify the use of spectrum. For unlicensed spectrum, a question is whether there will be sufficient spectrum available, in the future, as more and more devices start to use the already crowded globally harmonised 2.4 GHz-band, which seems to be the default for wireless personal area networks using technologies such as Zigbee and Wi-Fi.

Many M2M devices are less visible, but more pervasive, than personal communication devices, such as telephones and, therefore, raise issues in relation to privacy. Given the use of M2M for health, transport, consumer electronics, energy use, and virtually every other sector, a very large amount of information can be generated. Without appropriate safeguards, experience has already shown in some OECD countries, that privacy implications can lead to serious concerns for an M2M-service. Many aspects of the policy approaches identified in the OECD Policy Guidelines on Radio Frequency Identification (2008) will be relevant and could be considered as a starting point in addressing relevant issues related to M2M.

M2M will enable the collection, enrichment and distribution of a wide variety of data. Some of these data will be generated by the public sector and will be of use to the general public. Other data will be generated by private M2M-users and will be of use to public organisations. Adequate arrangements to give widespread use of data should be encouraged. For data gathered by the public sector, through M2M, the "OECD Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information" (C(2008)36) is of particular relevance.

Governments will be initiators of M2M use and large scale M2M-users themselves. By requiring the introduction of smart metering, or M2M for emergency assistance to automobiles or by using M2M to better support various public services, they will play an important role. Governments are therefore an integral part of the M2M ecosystem that will develop. Policy issues that need to be addressed are therefore are as much about the public sector shaping its role as about the government shaping the functioning of the market.

INTRODUCTION

According to some estimates there will be 50 billion mobile wireless devices connected to the Internet across the globe by 2020 and the total number of devices connected to the Internet in some way could reach 500 billion. This raises many important issues for stakeholders to consider. Economies and societies will be increasingly intermeshed with devices that continuously communicate with each other and provide information to users. That data will be processed and delivered as a myriad of signals across multiple devices and networks. This report aims to give an overview of the implications that this development will have for applications, business models and market structure as well as those for communication policy and regulation.

Different terms have been used to describe this development. It is known as the Internet of Things, Machine to Machine communication (M2M), embedded wireless, Smart (Living, Cities, Metering, Grids). Different titles that each describe the phenomenon in part, but have slightly different attributes or emphasis:

- The term "Internet of Things" is mainly associated with applications that involve Radio Frequency Identification (RFID). These make use of so called tags, tiny chips with antennae that start to transmit data when they come in contact with an electromagnetic field. They are passive communication devices, in contrast to active devices, that can transmit because they have access to a power source like a battery. These have been the subject of earlier OECD work.[1]
- The term Machine to Machine communication (M2M) describes devices that are connected to the Internet, using a variety of fixed and wireless networks and communicate with each other and the wider world. They are active communication devices. The term is slightly erroneous though as it seems to assume there is no human in the equation, which quite often there is in one way or another.
- The term embedded wireless has been coined, for a variety of applications where wireless cellular communication is used to connect any device that is not a phone. This term is widely used by the GSM Association (GSMA).
- The word Smart is used in conjunction with various words such as Living, Cities, Metering, Grids, Water Levy and Lighting to describe a variety of applications that make use of inexpensive communication to improve the delivery of services.

In this report the term M2M will be used, mostly in the context of the second and third description. Devices that are actively communicating using wired and wireless networks, that are not computers in the traditional sense and are using the Internet in some form or another. M2M communication is only one element of smart meters, cities and lighting. It is when it is combined with the logic of cloud services, remote operation and interaction that these types of applications become "smart". RFID can be another element of a smarter environment that can be used in conjunction with M2M communication and cloud services.

The main reason for the focus on M2M is to consider the implications for communication infrastructure and services. The other terms are too broad, too limited or too much focussed on a specific application. Many applications of M2M will make use of mobile cellular networks, because these are ubiquitous on a global scale, however not all devices will have wireless embedded. RFIDs play an important role, but as they are only passive, they will always need a communications device with an active component to query them and communicate the data onwards. Smart Living, Cities, Meters, Grids and so

forth, are applications with broader implications for economic and social development that are being considered elsewhere in OECD work.

M2M is enabled by ubiquitous connectivity

Machines with the capability to communicate are far from new. The speedometer in an automobile is a form of communication from a sensor reading. Strictly speaking machines communicating with machines are not new either. In factories machines are communicating information to control rooms, where control circuits may automatically react to that information. From the earliest days, in the use of information technologies, computers have processed signals from external sources. What has changed is that inexpensive electronics, the use of the Internet protocol, together with ubiquitous networks and (cloud) computing now allows any device to be equipped with a communications module. This enables devices to communicate status and information, which in turn can be aggregated, enriched and communicated internally or onwards to other units. This in turn allows the use of these data in new and useful ways. An example is to use the data gathered by the onboard computer of an automobile as part of the traction control system to tell cities where the roads are slippery.[2] The data was available to onboard computers in cars for decades, but with the advent of cheap communication it can now be communicated to others, combined and enriched.

Over 50 billion devices connected by 2020?

It is extremely difficult to estimate how many devices will be connected via M2M in the coming years. The 50 billion figure, mentioned at the start of this document, is a number that is widely cited and originates with the ICT firm Ericsson, which the company acknowledges is an estimate based on guesswork. By defining M2M as devices that have some kind of two-way communication, and that are not peripheral to another device, some types of applications can be excluded. A short range FM-radio transmitter, a keyboard and mouse, wireless headphones can all be excluded from the definition. Other applications like CCTV cameras can be included in the definition. Embedding 3G and 4G wireless capability in laptops, tablets and so forth may or may not be included depending on the situation.

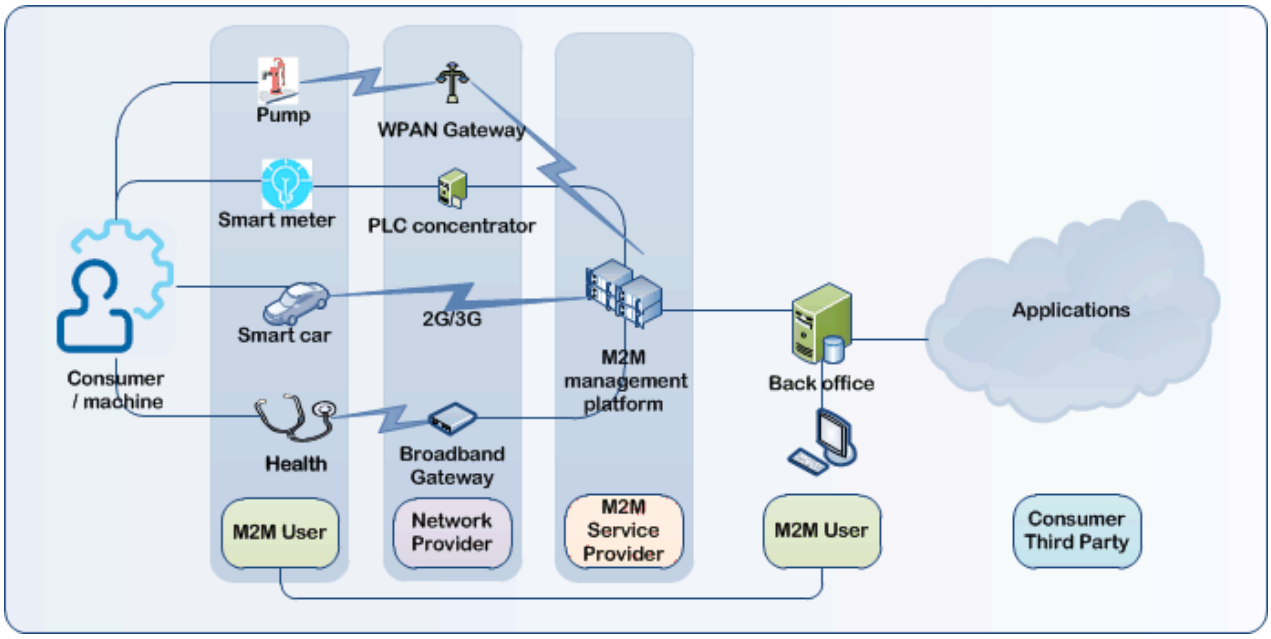
Berg Insight, a market research firm, estimated that by the end of 2010 around 80 million devices were connected using mobile networks. They suggest 290 million will be connected in 2015. Another company, IMS Research estimates that by 2015, 100 million devices per year will be equipped with mobile wireless connectivity with a 30% compound aggregate growth rate.[3] If these projections were considered together it would yield roughly one billion devices connected on mobile networks by 2020. As this excludes various wired and wireless solutions that do not use mobile networks directly, it is hard to say what the actual number will be. If, for example, every automobile produced had one communication device and had a lifespan of 10 years, this would result in around 700 million cars being "M2M enabled" by 2020. If every power socket in North America was "M2M connected" to a network, the number could be 10 billion. In the text and boxes, in this report, some data and estimates will be given that demonstrate why numbers can easily be doubled or tripled depending on the way connectivity is implemented for various applications.

Some firms using M2M, such as TomTom, Ford Sync and General Motors Onstar, and who use mobile networks, already have over one million devices under management. OnStar has six million customers, which make the number of devices it connects to mobile services larger than the number of mobile subscribers in Ireland, Norway and Slovakia.[4] The stated aspiration of TomTom is to have 20 million devices under management in 2015, which is more than the number of mobile subscriptions in 20 OECD countries in 2009.[5] For the purposes of this report it is not necessary to determine how many

devices will be connected across OECD countries and around the world. It will likely be substantial and almost certainly much more than current networks.

Policy makers increasingly recognise the potential of M2M for economic and social development. A growing number of governments have projects that make extensive use of M2M or that promote the use of M2M and are being used to evaluate its consequences. Some examples are the Dutch SPITS-projects for Intelligent Transport Systems, Brazil's SIMRAV anti-vehicle theft system, the European Union's "Internet of Things Expert Group" and the Korean government's "Master plan on the establishment of Internet of things" in 2009. The latter project includes development and deployment of public service models, such as monitoring services on M2M-based public facilities, weather monitoring services and intelligent metro bus stop services. Many countries are rolling out smart energy services, including metering and investing in eHealth, which may be supported by M2M. All indications are that the capability of M2M to support a range of services will ensure growth in its use by the public sector.

Figure 1. Elements of an M2M service and who controls it



Design of an M2M service

The main elements of an M2M system and value chain commence with a user or a machine. It may be, for example, that vital signs of a medical patient are monitored, or that the combination of a vehicle and its driver is monitored. These devices are controlled by an M2M "end user". This term does not refer to a consumer, but is the designation applied by standardisation organisation ETSI for the organisation that is formally in charge of the devices (*e.g.* in this sense, TomTom would be considered as the end user rather than one of its customers). This may be an automobile company, a utility managing drains and sewers and so forth. These M2M end users will need some kind of network to send the data back to their business systems. In between, for example, an M2M management platform that handles device specific tasks, such as fault detection when a device does not respond or management of SIM-cards, an M2M service provider manages the platform. The M2M end user will use the data collected in its back office systems. For example, to measure water in irrigation projects or glucose levels in diabetes patients. Some companies will open the data for further use by other applications either internally or under control of consumers and third parties.

Box 1. Velib, the bicycle sharing system of Paris

Paris operates the largest and most prominent bicycle sharing system in the world. Called Velib, it consists of around 20,000 bicycles and 1500 stations, or roughly every 300 meters within the city limits and some of its suburbs. The system is operated, for the city, by JCDecaux, an outdoor advertising company. The success of the Parisian system, based on the experiences of a similar scheme in Lyon, can in large part be attributed to the use of M2M technology. There are other bicycle sharing schemes around the world, but without a technological system to manage the bicycles and prevent theft, a great many of them have not been successful. The greatest problem for Velib is vandalism by non-users. The system used in Paris is now used in cities like London. Two elements are particularly noteworthy in the context of this paper, the use of two mobile networks to ensure coverage of stations and availability of the system and creating an application for users to make use of data about the availability of bicycles at every station.

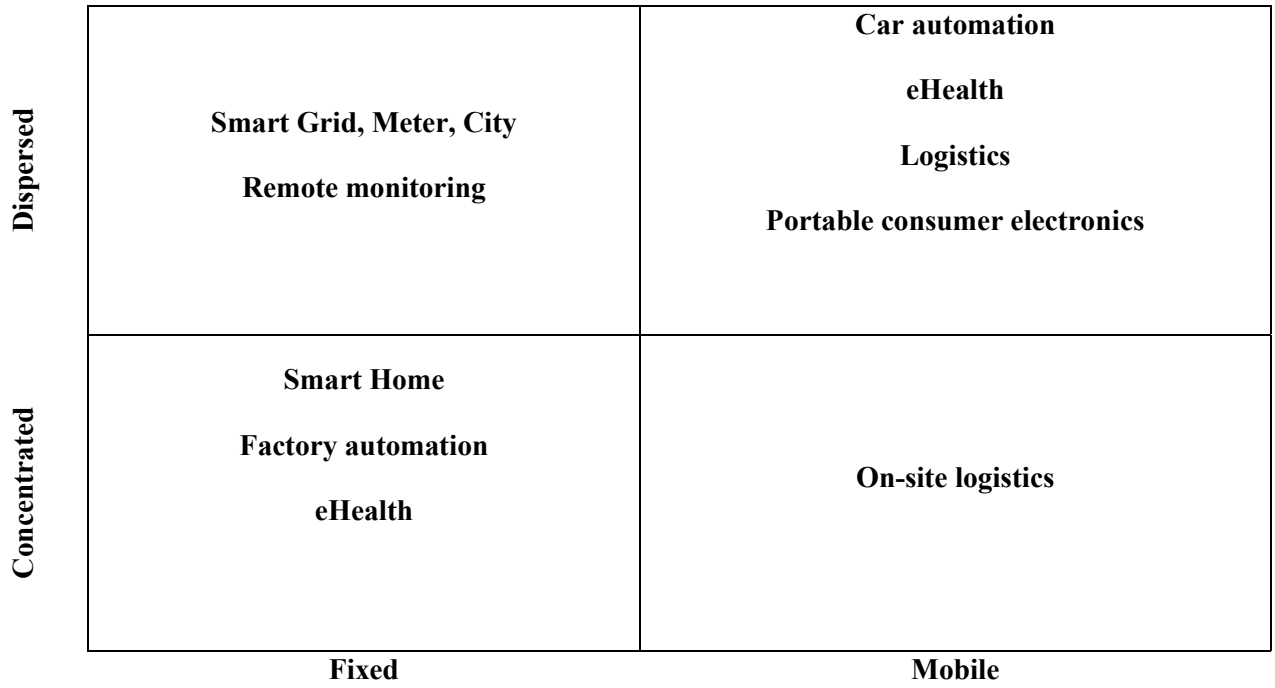
A daily, weekly or annual subscription allows a subscriber to rent a bicycle for half an hour at no charge. If the bicycle is not returned to a station within half an hour, EUR 1 is charged. Additional time incurs additional charges and this stimulates users to return bicycles and keep them in circulation. A credit card guarantee of USD 215 ensures that bicycles are returned. If a user wants to use a bicycle, they go to one of the many bicycle stations. Experienced users will use a smartphone application to check where the nearest station is and how many bicycles are available. Such a station consists of a terminal, where users can register and check their account information and 15 to 50 bicycle attachment points. They either register using their credit card at the terminal, or swipe their Velib subscription card, or Paris public transport card Navigo over the bicycle attachment point, which reads the RFID in the card. When the use is authorised the bicycle is released by the attachment point. The bicycle itself is only equipped with an RFID-tag, so the trip itself is not recorded. When returning the bicycle the attachment point reads the RFID in the bicycle and registers it. If a station is full, the terminal will indicate where other stations are and which one has attachment points free. Experienced users will use their smart phone application for this.

The bicycles are equipped with RFID and can therefore be identified. The people who have used the bicycles can also be identified through the RFID-enabled Velib and Navigo cards. The wide availability of 2G/3G mobile communications allows stations to be placed anywhere in the city and to communicate in real time. Every station is equipped with a single communication module and a SIM-card from a mobile operator. However, two neighbouring stations are connected to two different mobile network providers. If the system was only connected to a single network, it could potentially face problems with “dark spots”. The use of two operators at alternative stations also provides redundancy if one network is not in use for any reason. The attachment points are connected to the station using serial wired communication. This could be installed relatively easily because the streets had to be broken open to install the attachment points. A central system receives near-real time updates of the status of the whole network. The information is used to manage vehicles that redistribute bicycles around the service area. Redistribution is necessary as uphill stations see more bicycles checked out than checked in, as well as stations near major public transport nodes running out in the morning and overflowing in the evening.

The data on the location of stations, the number of attachment points free and bicycles is not just used for internal business processes; it is also used through two smart phone applications provided by JCDecaux and the city of Paris. These applications greatly increase user satisfaction and therefore use of the system.

The introduction of the Internet, wireless devices and cloud computing have greatly expanded the possible uses of M2M communication. The data collected can now be combined and used in a variety of ways. The same data may be used in different contexts on different devices. For example, municipal employees collecting refuse can be signalled by the container with regard to its volume and the date of previous collection. City administrators and ratepayers can monitor the efficiency of the service, as well as assist in the design of service improvements or the convenience of their personal use (*e.g.* are bins full).

Figure 2. M2M applications by mobility and dispersion



Dispersion and mobility define an M2M application

As the uses of M2M are as broad as that of human activity, it is not simple to classify applications. Using a vertical method of classification, based on application fields is difficult, as it would require describing every economic activity. This report therefore focuses on general characteristics that define an M2M application. The characteristics influence what types of networking technology will be chosen and what type of business models and regulatory issues may arise.

The types of M2M applications that are possible can be categorised by the amount of mobility and the amount of dispersion that need to be supported. Dispersion is related to the area that the devices are spread out over. When M2M is used in a factory or home setting, the dispersion of the devices is limited. If the devices are spread out over a city, a country or even globally, the dispersion is significantly increased. Mobility measures whether the device is stationary and can in principle be tethered or whether it needs to be able to move around and the extent to which it needs to be able to move around. As shown in Figure 2, different types of applications have a variety of needs in terms of networking resources. The clustering is approximate and it may be some types of M2M applications stretch over multiple quadrants. The quadrants can be used to distinguish the different demands that applications have stemming from business models and regulation.

Mobile and dispersed applications move around over large areas

Logistic applications are a good example of the use of M2M in a way that is both dispersed and highly mobile. For example, the tracking of ships, planes and trucks and the cargo they carry in containers has long been a basis for M2M types of applications. Not only is the location recorded, but also various parameters that are of interest to the owners of the goods, such as temperature, packing or other transport

conditions (*e.g.* whether the cargo is at the correct orientation or subject to knocks/blows that may cause damage).

The use of M2M in logistic applications is the basis for new business models and new forms of fees and taxes. There are several insurance companies developing Pay as You Drive models of car insurance. Not only do users pay based on the amount of kilometres driven, but also the way they drive and where they drive can be factored in the insurance premium paid. Governments are looking at similar technology to introduce road pricing, toll collection and taxation. More broadly there are many applications for transport efficiency and safety. The data gathered from navigation devices in cars, for example, can be used to provide information on traffic conditions. Other applications include automatic notification of emergency services in the case of an accident where a driver is incapacitated or disoriented.

Applications where M2M is used in a highly mobile and dispersed way include consumer electronics: for example an ebook-reader or a personal navigation device. Consumers expect these devices to travel with them everywhere they go. Some ebook-readers allow consumers to buy ebooks in almost any country in the world. The charges for roaming in these foreign countries are paid for by the vender of the ebooks. Some personal navigation devices communicate with networks to get real time updates about the locations of traffic jams, but also localised information for police radars, fuel prices and weather. One provider of navigation devices promises to reduce journey times up to 15% for their users because of the use M2M.[6]

Fixed and dispersed applications stay in one location, but are spread out

Many machines are located at a fixed location. Their owners want to monitor them for all kinds of information about the status of the machine or its surroundings. The use of M2M communications allows this monitoring. For example, alarm installations that have used M2M communication for a long time already. Other examples are the monitoring of sewer pumps, elevators, vending machines, copiers, ATM's and so forth. Until recently the use of these types of applications was limited to a single domain in a particular organisation, but new developments allow these devices to become interconnected. This allows their data to be combined with other data to create new services.

Box 2. Smart metering, smart grids

Electricity networks, for the most part, are currently hierarchically organised networks, where energy is generated in one location and then transmitted to a town or city, where it is further distributed to the consumer. Information on the consumer's usage flows back once a year when the meter reading is sent back. Experts expect energy production and distribution to be more localised and require much more information exchange. In order for this to be possible extensive use of M2M using fixed and/or wireless networks is required.

Smart metering is one of the first steps in a smart grid. The meter can transmit real time information on energy use, which the consumer can access in their own home and which the energy company can use to manage the network. Consumers could be stimulated to change their behaviour by introducing differentiated pricing for peak use and informing them of when such peaks occur. Furthermore smart meters can support consumers delivering their locally generated energy (*i.e.* through solar cells excess electricity back to the grid).

Consumer generated energy and other forms of local generation (solar, wind, combined heat power) can create new sources of imbalance in the network because their performance may be intermittent. Accordingly, to operate efficiently, the grid operator needs more knowledge of how much is delivered into a network. This requires constant communication to know where demand is and where production is available. New business models are also emerging where energy companies install solar cells on people's homes and the energy company manages all those cells together as one power station. The consumer gets a lower rate and the excess energy is sold on the grid.

The introduction of electric vehicles would also require the network to become "smarter". Parking spaces need to be equipped with a loading station, which needs to be able to support a billing mechanism. In addition, the use of electric cars could be an enormous burden on the grid, which needs to be well managed, especially during peak times for the most common working hours. In the morning, after people have driven to work, and in the evening, when they return home, there will be a major spike in demand for energy to recharge these cars. If it would be possible to manage this peak by distributing the load cycles during the day and night based upon the requirements of users this could save countries from building several power stations just to service peak demand. The energy stored in vehicles could also be used to level out the spikes in demand placed on electricity networks, for instance during the break in a major sporting event or popular television programme. These are known as television pickups and can be as high as 2800MW in the United Kingdom, or close to 10% of regular energy usage and as much as the energy of 4 power stations combined.

M2M communication solutions for smart grids need to work in fixed locations with little or no need for mobility. The solutions used would need to be able to support millions of devices. One meter per home/business and one to three more to allow for the charging of household cars and those of guests (not counting businesses, garages, etc.) If new business models take off, an additional communication device may be necessary for local generation of power. The European Union has mandated the use of smart meters by 2020 in Directive 2006/32/EC, which means there will be a market for around 180 million meters at a rate of one per household. If we assume most OECD countries will follow, then this market alone could be around 400 million units, at one unit per household. If electric cars really become the vehicle of choice for the future, around one billion M2M communication units would be necessary in the OECD region to co-ordinate charging these cars.

Fixed and concentrated applications are in one location and stay there

Many applications for M2M are found inside factories, offices and households. Most machines in these locations have some way of reporting their status. In many factories a level of integration has already been reached, so that the control room can manage every element of the production process. Offices and residences, however, may have devices that can report on their status, but there still is little integration available. Even though it is possible to control an Internet protocol enabled thermostat remotely in a home or to have a IP-enabled fridge that records the food it contains (and this has been shown in science fiction since the fifties), in practice most people do not have such an application. It is mostly in the area of entertainment that we now see types of M2M, for instance music players that are controlled by mobile phones. More and more TV's and entertainment systems are connected to the Internet, though this might not yet fit the definition of machine to machine communication. The promise of a smart home, where the

home and its appliances are equipped with sensors, communicate and can be remotely controlled, however remains alive and there are do-it-yourself projects on the Internet available, like those built on the open source platform "Arduino", that show some of the possibilities such as: monitoring a garden through various sensors and operating indoor lighting and a plant that signals whether it needs water through Twitter.

It is in the home where many applications for eHealth are expected to see their use. One example is an alarm system for the elderly, complete with voice and video options if the alarm is activated. At this moment alarm systems are plagued with false alarms. The combination of voice and video would allow for verification and a more appropriate response in the case of an alarm. Remote monitoring of the functioning of specific organs or, for example, blood sugar levels are applications that may need more mobility and use over a wider area and would therefore fit in the other quadrant (in Figure 2).

Mobility at a specific location

M2M applications that need mobility at a very specific location are mostly concentrated around on-site logistics. Such a type of application can be a fully automated container terminal, where robots unload ships, pick up the containers, move them to and from storage locations and load them onto trucks, trains and ships. Automated warehouses are a similar application. Hospitals are another location where mobility is needed in a concentrated space, monitoring the patient while she moves through the hospital and supporting various logistical processes in the hospital.

NETWORKING TECHNOLOGY AND M2M

In this section the advantages and disadvantages of using various forms of networking technology for M2M applications will be discussed. It will show that the options for networking technology can be distinguished by mobility and dispersion, similar to applications. By no means is this paper meant as a definitive guide to all proprietary and standardised networking technologies that are available. In many areas there is a very competitive market place, with competing public and proprietary standards. For regulators, however, it is necessary to understand the different architectural choices as these influence the costs of deploying an eHealth solution or other M2M application. In addition, choices taken today may influence spectrum policy for decades to come or change the roles between suppliers and customers in mobile networks. In the next chapter these architectural choices will be combined with business models.

Figure 3. Dispersion and mobility define technology choice

	Fixed	Mobile
Dispersed	PSTN Broadband 2G/3G/4G Power line communication	2G/3G/4G Satellite
Concentrated	Wireless Personal Area Networks Wired networks Indoor electrical wiring Wi-Fi	Wi-Fi WPAN

The various technologies will be discussed starting with those that support the most fixed and concentrated type of applications and goes on to the mobile ones that are dispersed on a global scale.

Requirements for M2M communication technologies

An ideal M2M communication technology would allow instantaneous secure access to the Internet anywhere in the world at any speed. It would work equally well indoors as outdoors, it would have unlimited range, zero latency and unlimited throughput, while costing virtually nothing and consuming no energy. It would provide access and management to data necessary to use M2M efficiently while ensuring the protection of privacy. Unfortunately this is not the case and therefore all technological choices are tradeoffs. It is these trade-offs that can make the choice of a networking technology challenging. For smart meters, for example, the industry has looked at wireless personal area networks, wireless mesh technologies, piggy backing existing networks, CDMA450, GSM/GPRS and powerline communication.

Some general requirements and associated trade-offs are:

- Range and penetration: the more range and better penetration of walls, windows, foliage and so forth. the easier it is to deploy in a wider area, but range is inversely correlated with power consumption and throughput.
- Power consumption: the lower it is the better for battery-operated devices. But lower power use often results in lower throughput and range.
- Throughput: the higher the throughput the better it is, however this is often inversely related to battery life and area covered.
- Number of devices supported: the more devices that are in a particular area the more they need to share resources, which affects performance.
- Types of network supported: star, mesh, tree, peer-to-peer are different topologies, each with its own advantages and drawbacks in terms of usability, throughput range and so forth.
- Ease of roll-out and maintenance.
- User interaction: if users need to configure the device and the way it communicates this creates a hurdle. Ideally, M2M is switched on and it works.
- Open or closed: whether the data is available only to the owner of the device or if others need to be able to interact with it.
- Expected lifetime: a device that is equipped with M2M can have a 20 year or longer lifetime and ideally the M2M solution remains the same.
- Local and global use: some technologies can only be used in some countries, because of regulations or technical issues.
- Types of applications supported: Most technologies are designed with a specific set of use cases in mind. M2M, however, scales from short messages sent once a month to complex interactions supported by voice and video.
- Mobility: whether it will work at any speed or any location/environment in the world.
- Failover capabilities: If a network fails, users will want a backup solution.
- Multi-protocol support: the support of multiple networks would allow to choose the network that best fits the situation.

- Security and privacy: M2M, in a potentially pervasive manner, will generate data that pertains to individuals and their private lives.
- The existence of case studies and experience with scale: not every technology has seen equal implementation in a large scale. Often new constraints show up when the scale is increased from a pilot to actual implementation.
- The availability of vendor solutions; new technologies often have desirable qualities but come at the cost of having less suppliers, which may lead to longer lock-in.

The above list is lengthy and could be longer. What it does show is that choosing the right M2M solution is not as easy as just bolting a communications device onto a machine. The way the system can work, whether it is "future proof" or not and whether it can accommodate changing demand depends upon these choices. Some M2M projects already fail at the stage of choosing what parameters are important, others when changing demand invalidate past choices. Smart metering for instance has seen a large number of pilots, but no market consensus on what communication technology is the most optimal. Companies have found it difficult to find a single technology or group of technologies that satisfies all demands that a smart metering project has.

For policy makers it should be clear that when relying on M2M in some form to support policies, there are trade-offs and these trade-offs impact the viability of the project at every level.

Indoor electrical wiring

Many devices in a residence or business are fixed in one location and are not portable. In these cases there may be a single network that connects them all. Devices such as washing machines, air-conditioners, central heaters, may all be connected to a single electrical network. With M2M, not only could the machines that are connected to a network communicate, the sockets and the plugs themselves could communicate.[7] There are many companies that are pitching products and ideas that they say can make homes and businesses measure and save energy use, prevent overload and fires and protect children. Other devices already use electrical networks to extend the range of communications equipment, for example, using standards like X10, Universal Powerline Bus and the HomePlug standard.[8] With 10 billion electrical sockets in North America alone, there is an enormous potential to create communicating devices that use indoor electrical wiring.

The benefits of using indoor electrical wiring are that virtually all households are already equipped with it. The network can also carry a wide variety of signals and deliver bandwidth of up to 600 Mbit/s. Implementation can be as simple as plugging in a device or plugging a new M2M-enabled socket in the existing socket. It can work well with existing standards like Ethernet, which is the dominant Local Area Networking technology, which allows interaction with other in-household devices connected to the same network. Communicating to devices and networks in other homes or the wider network over the electrical network is not possible as the signal cannot go past the meter.

Wired networks

There are a variety of standards that support networking using wired communication. The default standard for computer networks today is based on the IEEE 802.3 Ethernet standards, that support anywhere from 10 Mbit to 100 Gbit over twisted copper and fibre based networks. There are also other standards in use, like serial communication, which have specific backgrounds in, for example, industry

automation. The advantage of wired networks is that they are much less susceptible to outside interference compared to wireless networks. As a result the speed of the network is better guaranteed. A significant drawback is, however, that a wire needs to be connected to the device, which will require work and costs, greatly limiting the range of locations it can be in and the ease with which new sensors can be added.

Wireless Personal Area Networks

Wireless personal area networks (WPANs) is the generic term for short range networks. There is a wide variety of standards to choose from; some public, like (low power) Bluetooth, Dash7[9], Wireless USB and Zigbee, but also proprietary like Z-Wave, ANT and Peanut. These technologies aim to bring communications ability to a wide variety of devices allowing users to do away with cables and offer some mobility. They are incorporated in smart meters, home automation, mobile phones power sockets, keyboards, cars, tires, outdoor sensors etc. Depending on the technology they offer different advantages with regards to range, penetration, throughput and power usage (manufacturers promise up to 10 years of use on some batteries).

The major benefit of using WPANs is the low power combined with the lack of wires. Depending on the technology used and the situation it is used in, the range can be anywhere from 1 to 100 meters. Some WPAN networks allow the possibility to use the network in mesh configurations, which allows for direct interaction between devices and the extension of range. However given the myriad of possible standards, it does seem that there is not really a uniform standard yet. This is confusing the market place, which is exemplified by the market for home automation, where each technology is claiming to be the solution, but there is no uniform (or multi-protocol) solution.

WPAN based devices will need a relay or a concentrator to connect to the wider Internet, the cloud or other devices in the same network that are out of reach. This relay or concentrator will need configuring.

PSTN

The public switched telecommunication network (PSTN) has been used in many ways to support older versions of M2M communication. It is used for alarm installations, electronic payment terminals, elevators and many other applications. The main reason for using the PSTN is its ubiquity, ease of use and high availability. Drawbacks are that it does not support high bandwidth applications and a connection needs to be setup. One of the problems associated with this use is that some of it is using the PSTN in ways that may not have been envisaged by the network operator. When the network operator upgrades the network to, for instance, VDSL2 and a system where all phone calls are converted to VoIP, the M2M service may not function anymore.

Wi-Fi

The IEEE 802.11 family of standards, known as Wi-Fi, is one of the most successful networking standards. Originally designed for connecting cashiers to networks it is incorporated in almost any laptop, smart phone and more and more peripheral equipment. It allows devices to connect with speeds ranging from 1 Mbit/s to 600 Mbit/s over ranges of up to 250 meters. Its use in M2M equipment is however limited as it is considered to demand too much energy. This means it either needs a permanent source of electricity or a battery that can regularly recharge itself. Like WPANs, a user needs to configure the connection to the Internet. Even though many consumers now use some form of Wi-Fi in their residence, connecting M2M devices is not as simple as it may seem, because depending on the situation the device will need to know a

different password to access the network, which will need to be entered into the device through some means and understand various implementations of Network Address Translation.

Broadband

Technologies such as DSL, cable and fibre are the broadband networks of choice for most consumers. Broadband itself is not used in most cases to connect directly to an M2M device. Generally, it is the network of choice to carry the bits from a WPAN, Wi-Fi or electrical wiring network to the Internet. Broadband is an important enabler in allowing M2M to deliver on its promise. An area that broadband still needs work on is the ease with which users can connect devices to the network. An example will illustrate this point.

In delivering a health service over a user's broadband, the health service provider has to ask questions regarding the following:[10]

- Will it make use of the broadband connection available at the customer's or use a (dedicated) wired or wireless network? Is broadband available?
- Is the customer connected to broadband? If not will the health service provider provide a connection?
- Is the customer's connection sufficient? What if an upgrade or a different subscription is needed?
- Will the service work with any Internet Service Provider or only with specific ISPs?
- Is it easy to connect to the customer's broadband connection? Who will install and configure the wired/wireless network: the customer, the health service provider or the ISP?
- Who is responsible when the connection malfunctions or changes influence the delivery of the service?

Though very practical in nature the issues further complicate the development of new M2M services on broadband networks. It certainly is not "plug and use" like plugging an electrical device into the electricity network.

2G/3G/4G mobile wireless[11]

Digital mobile wireless technology, around the world, is by far the most successful communications technology in terms of the provision of access. In 2010 an estimated five billion people had a mobile phone. Technologies used are GSM, GPRS, CDMA, UMTS, Wimax and LTE (in the future) and related standards. For M2M applications mobile wireless offers both the possibility to be used in a dispersed as well as highly mobile set of configurations. It is, in many ways, the technology best suited to many M2M applications. Its appeal comes from some of the following:

- Near ubiquitous global availability anywhere, where people live.
- Centralised control through the use of SIM-cards. This allows instant activation without user interaction.
- Support for roaming between networks.
- Reasonable coverage indoors.

There are some drawbacks to the use of mobile wireless technology which should be taken into account when designing an M2M solution based on it.

- The coverage for 2G technologies is pretty much universal. Coverage for 3G is in most countries limited to denser populated areas. 4G is not widely available; though roll out will happen in the coming years.
- Dark spots can be a considerable problem for static deployments. At these locations the network will not be able to deliver service for a longer period, even though the network is available. The dark spots will exist more indoors than outdoors, but can be everywhere. During the lifetime of an M2M deployment a small percentage will experience a lack of coverage at a location for longer or shorter periods of time. When deploying hundreds of thousands of devices, this is a significant number.[12] It is not known where and when the dark spot will occur and how long it will last. Being able to roam on multiple networks significantly decreases the chance of dark spots occurring. Some operators offer this solution for their customers, by using a foreign or international SIM-card.
- 2G networks are scheduled to be decommissioned and replaced by 4G networks in the coming five to 15 years. Building an M2M solution that only functions on 2G may not be future proof. However, there are very few or no 4G modules available and it is not expected that 3G coverage will become universal. The consequences of this, for market development and potential regulation, will be discussed in later sections.
- Standard SIM-cards are prone to theft from M2M devices and are prone to failure in harsher environments, *i.e.* with significant vibration or temperature differences. Soldering the SIM-chip on a board is preferred in such situations.

Policy makers need to consider these drawbacks, as they are the result of today's approaches and may significantly influence the future options available for policy making in the coming years. The drawbacks are further influenced by the way the mobile industry functions to provide today's services relative to future requirements for M2M services. Policy makers can have a positive influence in the usability of this technology for M2M-users. This will be discussed in later sections.

Power line communications

Power Line Communications (PLC) is used in the context of smart meters. ENEL, an energy provider in Italy, has used it to connect 32 million households and businesses for remote meter reading. Given the ubiquity of the electricity network and the technical possibility to transmit signals over it, electricity networks hoped to make use of it. Because all nodes in an electricity network receive the same current, all nodes will also receive the same signal. There is significant distortion on the line to this signal, because the network was not meant to be a communications network, which makes it necessary for intermediary nodes to retransmit the signal several times before it has reached all nodes. In this sense the network functions as a mesh, where nodes will retransmit signals that are not meant for them. Consequently, there are some significant drawbacks that will result in a limited use for PLC in smart metering. These are:

- It can take up to 24 hours before all nodes are queried in layouts of several hundred nodes.
- No ability for real-time messaging. Relaying messages to nodes and back, *i.e.* to measure its functioning or read the meter can take considerable time, because they have to be entered into the schedule of normal queries. This also makes it a less likely pick for smart grid applications.
- Networks need to be rolled out all at once. It is not possible to cherry-pick locations, based on customer preference, or to await the demolition or building of a particular part of an area. All nodes are necessary to carry the signal.

The conclusion of the drawbacks section is that the network cannot deal well with any changes in demand beyond meter reading and therefore will not enable future innovation.

Satellite

Satellite communication is used for M2M applications in areas where land based networks cannot offer a economic alternative. It is used in telemetry, logistical tracking and remote monitoring. There are a wide variety of satellite networks to choose from across OECD countries. Some have full global coverage, others offer connectivity in a particular region. Even networks that were originally built for voice applications only, like Iridium, are now used for M2M. Other networks like Lightsquared, in the United States, are relying on a hybrid model, where land based wireless networks are combined with satellite communication. The main drawbacks of the technology are:

- The need for line of sight to the satellite, which makes it harder to use in urban and mountainous areas (this is similar to the darkspot problem of mobile wireless technology)
- Bulk of the equipment
- Low data rates

Despite the drawbacks, it is the only technology that will function in many remote parts of the world and at sea.

Authentication methods

The previous paragraphs discussed access to networks via various networking technologies. Access cannot work without authentication.[13] The owner of the network will want to control who can have access to the network. An explanation of how authentication functions is important to understand issues regarding access to the market and regulation of the market, which are discussed in later sections.

In order to give a device access it has to have a unique identity. To verify identity an access technology needs to be based on three principles:

- What you know; a secret only known to those that are trusted.
- What you have; something tangible, only in the possession of those who are trusted, like a letter or a ring.
- What you are; a physical trait of the body, like the iris or fingerprint.

What you are is, in the context of M2M, less relevant, but the other two elements are an essential part of security systems.

Box 3. Connecting the car

Automobiles have been the focus of many M2M initiatives to improve its use and usefulness to users and owners, or as a way to realise a public goal. Some examples are:

- eCall, an initiative by the European Union for emergency services in cars.
- OnStar and Sync are examples of services offered by vehicle manufacturers to car owners, varying from theft protection to navigation and emergency services.
- Saab has demonstrated a car equipped with an Android powered tablet, that would let users install a variety of apps from an appstore and monitor thousands of car parameters, which in turn could lead to new Internet services related to the car.
- The Brazilian government has required new cars to be equipped with the SIMRAV anti-theft device, which makes use of GSM to track a car.
- Pay as you drive insurance is available in some places and makes use of vehicle tracking using GPS and M2M.
- Several OECD governments are looking into dynamic road pricing using GPS and M2M enabled solutions.
- Companies are using GPS and M2M for fleet monitoring, not only to know location and speed, but also freshness of cargo and use and abuse of vehicles.
- Navigation devices are more and more equipped with M2M communications for real-time updates.
- Onboard entertainment in cars is an area that could benefit from M2M technology.

What is interesting is that these systems are not necessarily integrated into one system. Some may be installed during production, others post-production. One car may therefore be connected with multiple communications modules and multiple SIM-cards, each under the control of a different company.

In order for a device to be unique it needs to have a unique number. If the number is not unique, the network may make a decision for one device and impact other devices that have that identity. In order for identities to be unique some type of registration needs to be done that guarantees uniqueness. Unfortunately, without some centralised control of numbers that is enforced by network operators and/or governments, keeping identities unique has turned out to be rather difficult. Some identifiers that have been used in networks, but that are often copied, cloned or forged are Ethernet MAC-addresses, IMEI-numbers[14] that identify mobile handsets and similar numbers. These numbers are therefore not a good basis to identify a device by.

To avoid duplication of IDs network owners will have to make use of numbers from reputable sources that have a way to enforce that the identity is not cloned, copied or forged. There are different sources that M2M users turn to:

- A self-administered pool of identities. This is the route generally chosen, when the identity is not used in the network of a third party or issued by a third party.
- A trusted third party: an entity that is recognised as an organisation that can verify the identity and uniqueness of a user for instance when a certificate is used.
- An industry body: This is a trusted third party that issues numbers to various market players. This can work well if the participants have some way of enforcing the uniqueness of numbers and to punish those that do not follow rules. For example, domain names and IP-addresses are unique because traffic will not arrive or other networks will block a network and/or host repeatedly or maliciously assuming an identity that has not been assigned to them.
- Governments: Governments assign various numbers for use in telecommunications markets. They have a variety of legal instruments to further back up industry enforcement. Government issued

numbers are for example telephone numbers (E.164) and IMSI-numbers (E.212) that identify mobile subscribers.

Sometimes identities are "stacked". An M2M device may be identified by two or three identifiers. For example, a user of an ereader may have a personal identifier that is used for multiple devices, so that books can be bought and read on every device the user owns (PC, tablet, ebook-reader). The reader may have a temporary or permanent IP-address and the device may have a telephone number and IMSI number to be able to make use of the mobile network.

In order to be authenticated on a network a device can make use of a username and password; this is known as single factor authentication. Passwords have as a drawback that if users enter them, they are often easily guessed. In order to make it less easy for an attacker to get access to the username and password encryption is used. Every user may get a unique encryption key in the form of a certificate. The combination of user name, password and a certificate is more secure than just username and password. However, some security experts argue that if the memory of the device is not securely shielded, it is possible for an attacker to read the certificate and the other credentials from the memory. In their opinion adding certificates is more like adding a longer password than adding a new layer of subscription.

In order to make the authentication even more secure, bankcards, credit cards and SIM-cards make use of a chip-based authentication method. The chip carries the identity; a number, passwords and one or more cryptographic keys. To this is added a specific design of the chip that is unique to the particular organisation that the chip is made for. This is known as two factor authentication, as it requires both knowledge and a physical device. The chip will process a series of questions and answers based on the keys and identity on the chip and some that are provided by the network; only when the answers to all the challenges are correct is the device authenticated. To this can be added that the organisation the chip is made for does not know the particulars of the chip or of the keys stored on the chip. Only the producer of the chip would know this and will load this into a secure authentication device in the organisations network. In a mobile network this is the HLR. If done well, the attacker would have to physically analyse the chip under an electron microscope and understand all the particulars of the authentication and then either copy the chip or build an emulator in software.[15]

M2M devices may use any of the aforementioned authentication methods. However, a form of chip-based authentication is considered the most secure. It is for these reasons M2M users are looking to apply SIM-cards as authentication methods; next to not having to reinvent such an essential element, the option to use multiple types of networks with one type of authentication becomes possible. There are for instance already standards to use SIM-cards for authentication access to Wi-Fi-networks. The use of standard SIM-cards is however controlled by governments through the administration of the E.212 numbering plan, so governments need to be aware of this development for their numbering policy and for any future liberalisation of the market.

Summing up the technologies

There is not one technology that fits every requirement for the efficient use and economic development of M2M. What is clear from the consideration of the various technologies is that 2G/3G/4G wireless meets many objectives, for different uses, as it can be used in both fixed and mobile situations with a wide dispersion. Its security architecture is such that it can easily be rolled out on a large scale without needing user interaction. In the next section 2G/3G/4G will be the technology with the most focus on it. It is here that M2M has a number of challenges stemming from existing business models and regulation. A move to another communications technology is not simple as none of the other technologies can easily replicate its usability.

The other technology to keep in mind is WPAN-technology. It has superior duration on a single battery charge and can be embedded inexpensively in many devices. However WPAN is still a very open area for competition between standards. The lack of a standard or multiprotocol support makes it hard to choose the right technology. This is a potential problem for policy makers, who wish to be technology neutral, but also may be required to make some kind of technology choice, if that selection has not already been made by market forces. For example if a country mandates that a smart meter should be able to provide real time information on energy use to indoor devices, this is almost certainly done using some form of WPAN communication. But who will choose the winner? Will it be the meter supplier, the energy companies or the government? The viability of a market for consumer devices that make use of smart meter data would benefit from uniformity and interoperability. If the rest of the world chooses a different technology the country may have a significant investment in a more expensive or ultimately inefficient legacy system.

To be sure, all other technologies each have their specific applications. However, they will mostly be limited to niche applications whereas WPAN technology will most likely dominate the indoor and short range applications and 2G/3G/4G will dominate the market where dispersion and/or mobility is required.

Access to a unique and verifiable identity is another important requirement for many M2M applications. The model provided by SIM-cards seems to offer a great deal of flexibility and possibilities. There are other ways of providing a secure identity, but using a SIM-card chip soldered onto a motherboard or integrated into a chipset appears to be a very cost-effective method of providing security. As regulators play an important role in assigning SIM-card numbers (so called IMSI-numbers) they will have to take this role into account in terms of the future of M2M. Some discussion of this has already taken place at the ITU's Study Group 2 and the CEPT/ECC. The Dutch Ministry of Economic Affairs commissioned a report by Logica on the topic, which will be discussed in later paragraphs. It is expected that both the ITU and CEPT/ECC will give the topic more attention in 2012.

THE IMPLICATIONS OF M2M ON BUSINESS MODELS

If the market, as expected by many players, aims to introduce billions of M2M devices, there will be a need for stakeholders to assess the costs and benefits of existing business models. Recent experience in communication markets has demonstrated that there may also be a need to develop new business models. Not only will there be innovation in services related to the devices, there may need to be a redefinition of the business model of communication companies to facilitate a new type of customer. A consumer-oriented communication company, with millions of customers in a single country each owning one or more subscriptions, may be required to adapt to deal with single customers with millions of devices across many countries or continents. The demands by M2M customers on communication companies, in terms of management, roaming, coverage and provider switching are very different than what is currently the norm. It is also likely that some common regulatory measures, to improve competition in the market, such as through enabling lower switching barriers, may not be sufficient and alternatives could be necessary. The proposals for alternatives are discussed in the next section and focus on removing elements from regulation that prohibit large scale M2M users from entering the wholesale market for mobile communication.

New business models enabled by M2M communication

M2M can allow companies to improve existing processes, by allowing remote monitoring, sensing and real-time updates, whereas before these were based on site visits, calls from customers, or monthly status reports. This may, for the most part, be incremental innovation, such as by cost reduction. There will, however, also be new business models, enabled because processes can be implemented in ways never used before. Some examples of these new business models enabled by M2M are:[16]

- Pay as you drive insurance: The amount of risk associated with driving (and therefore the amount of the insurance premium) is a function of distance driven, location, time of day and driving style. In the past there was no reliable way to measure these variables. Now that these variables can be measured, it is also possible to make insurance products that factor in these variables and increase or reduce premiums based on use.

- Digital content distribution: First generation ebooks required the transfer of content downloaded to a PC on to an ebook by means of a cable or a memory stick. This was a cumbersome process that required multiple steps and planning. Some newer eBook models have a 3G mobile phone embedded. This allows the purchase of content straight from the device and the distribution of periodic content (*e.g.* newspapers, magazines, blogs) to the device. The connectivity is provided by the eBook distributor at no cost to stimulate and improve opportunities for sales. Similar business models can be envisaged with digital music/video players that have 3G provided by the likes of Spotify, Amazon or iTunes and allow subscriptions and streaming of content.

- Products as services: Today's economy is already known as a services economy. M2M will allow this development to be extended further. Already there are companies delivering light as a service (charging by the lumen) or companies that aim to make energy-saving a service, receiving a payment based on the savings they realise. M2M features heavily in these business models.

Combining new information with real-time communication enables these new business models.

Box 4. Let the buyer beware

Buying M2M services is not easy for companies. The industry has many examples of problems users encountered. By way of example: A smart metering initiative, that after five years had to renegotiate its data contract and heard that the data price was increasing instead of decreasing with the general trend. Its provider knew the company would not be able to move suppliers. Another company agreed to a contract where there was a clause that said that data use would be rounded up to the nearest 50 kilobyte. What the M2M user did not understand was that this was per message and so every message was charged like it was 50kilobyte of data. A third M2M user wanted mobile information screens throughout the country. Not being able to secure a favourable data rate from its network operator for the expected 100-200Mbyte of data traffic per screen, it resorted to buying a few hundred consumer SIM-cards for telephony that came with an 'unlimited' data plan.

Business requirements for M2M

The requirements M2M providers have, for M2M applications, are significantly different from what consumers and business ask from their communication providers for standard telephony and data for users. Normally, in the case of mobile wireless services, a user is charged per device/SIM-card, according to the type of subscription bundle they have taken from a network operator. In principle the user does not want to interact with the operator too much. Contact is mostly over a bill, or a configuration issue. A helpdesk, in the case of the latter, handles this on a per device/user basis. The consumer has to accept more or less the parameters (roaming networks, coverage and so forth) of the service as a given and cannot change too much of it. In order to change parameters, a change in provider may be necessary and this can be done, for example, by switching a SIM-card.

M2M users have completely different demands on their communication suppliers. Their demands come from a perspective where thousands to millions of devices have to be managed remotely by a limited staff. In order to manage these devices effectively their interactions with the network operator are different and often at odds to the way network operators work today. Some of these demands are operational, others are monetary, some of these may look the same to consumers, but are different in practical application. Standardisation organisations like 3GPP and ETSI have identified these needs and are working on standards to deal with some of these requirements. Other issues raised come from a study for the Dutch government, by Logica, on M2M for which industry experts were interviewed. Examples are:[17]

- Full insight into the status of the network, so that in case an M2M device does not communicate it can be verified whether it is a network malfunction or a device malfunction. Calling a helpdesk with a list of numbers is not a practical solution.
- To be able to switch mobile networks at the end of contracts or in case of disputes, but without having to switch SIM-cards.
- To choose another network, at will, if a network has downtime or a darkspot, from one mobile network to another.

- To activate a device only when a customer has bought the device and activates it and if necessary provide credentials like IMSI's and keys only then.
- To be able to negotiate roaming charges directly with local operators and change to a local network of the M2M users choice when crossing a border.
- To have a single subscription with one bundle for all devices, instead of a bundle and subscription per device.
- To have seamless access to home gateways, which can also act in combating the effect of darkspots or in offloading traffic to fixed line or fixed wireless broadband networks.
- To have guarantees on the expected lifetime of the communications technology.
- To have controls to stop communication in case of theft of the device (or the communications module).

Given the wide range of possible applications and the different ways of billing for these applications, every M2M user will have different demands on their supplier.

Fulfilling the requirements is challenging for mobile network operators (MNOs)

The list of requirements that M2M users have is quite extensive. For many MNO's the systems aimed at supporting service to consumers are not capable of meeting the demands of M2M users. The billing systems are for instance not ready to deal with a subscriber that has one bundle for ten thousand devices. The result may be that if an M2M customer makes use of such system, it will have to predict at the start of each month what the data usage of each device will be and shift the devices between low, medium and high usage subscriptions. An example of a consumer electronics company that needed to do that for its devices was reported in the Logica report. Seamless access to home gateways is another issue that is not available yet. MNO's do not know how long their 2G networks will be in operation. Access to the wholesale market, for example, to negotiate roaming is not possible at this moment for M2M end users. It can be seen from the offers by services such as ebook readers and in car services that the commercial reality of international data roaming is such that it cannot transparently and uniformly offer the same service to its customers in every country.[18]

The market is expected to solve many of the problems mentioned above. Some mobile operators have set up dedicated business units that only work on M2M issues. These units behave much like MVNOs on the MNOs network and have a different billing system, home location registers, different interfaces into the network and can deliver to customers what is demanded (at least in the home network). Some operators have developed their systems from the ground up. Others are sourcing them from specialist M2M mobile service providers, like Jasper Wireless, who work with AT&T, KPN and Telefonica. Customers should be able to expect items like billing, access to home gateways, activation and insight into the network to be solved in the near future.

The difference between large and small MNO's becomes apparent because of M2M. Smaller or more regional or national oriented MNO's are seeing the M2M market as an expensive market to get into; with low returns on those expenses as the average income per SIM is one to five dollars. Furthermore they have difficulty replicating the coverage of larger multinational MNOs. Even if they could put a better offer on the table than an international MNO, they often will not be contacted for larger transnational M2M projects. These MNOs will have to find a different mode of competition if they want to compete with

larger multinational MNOs. They will either have to join an alliance of some kind or find a way of dealing more directly with the M2M end user.

Business requirements will result in paradigm shifts

M2M customers not only have different demands than consumers, because of their size they may also want to play a different role in the market. In most markets, including the one for Internet connectivity, if a business's activities grow beyond a certain size it will enter wholesale markets that before were not cost effective to enter. To give some examples:

- Content providers will opt to become an independent Internet network, once they can save enough money on transit by peering directly with other networks.
- Companies will buy and sell electricity or gas wholesale once this is cost effective. Some will even build their own power generation stations and sell excess capacity on the market.
- Supply chains are a combination of internal and outsourced activities. Companies will mix and match solutions where they fully own and operate the logistics and warehousing with outsourced solutions managed by third parties, *i.e.* situations where international shipping is done by third parties and local distribution is done by the company itself.

In the mobile communications markets it is not easy to enter into wholesale markets and mix and match offers based on needs, competences and availability. The market structure determines that the mobile network operator determines all operating parameters.

In mobile networks in every device there is a SIM-card that is owned by the mobile (virtual) network operator.[19] The SIM-card authenticates the mobile device making mobile networks secure and easy to use with little or no user configuration necessary. It also makes switching between mobile operators as easy as switching one SIM-card for the other. As a result it was the basis for competition in the mobile network market. The result is that no change can be made without either the operator making the change, or without changing the SIM-card. The M2M user will not be unique, but will look to the network just like other customers of the operator. This is problematic for M2M users with thousands or millions of devices when:

- Switching mobile networks, the SIM-card has to be switched in order to make the switch possible – switching physical cards requires complex logistics and a great deal of staff time. Number portability is in this case not sufficient as the E.164 telephone number will have to be associated with a different operators E.212 IMSI-number that is unique to the operators SIM-card. As a result it is impossible to switch operators without switching SIM-cards, though the E.164 phone number may be retained.
- Using multiple networks or switching networks during downtime, most networks are designed to refuse to connect devices of national competitors, so national roaming is not possible and in some cases regulation explicitly precludes it. Using a foreign SIM is sometimes used to bypass this problem as it generally does allow national roaming, but comes with cost problems.
- Using one global supplier: there is no network that has global coverage and most do not have a network that covers all countries on any given continent.
- International roaming, the customer is dependent upon the roaming contracts of the provider of the SIM-card. These may be inexpensive for one nation, but can be expensive for another.

- Getting access to home gateways is dependent upon contracts that the wireless network has with broadband providers. These broadband providers may be in a group with competing mobile networks and may therefore only have limited incentive to provide services. In practice that means that even if an M2M user could negotiate a deal with a network for access to a home gateway or to switch a mobile network, in practice this is not possible.

Box 5. Consumer electronics and M2M

Never without a book, that is the promise of the ebook reader. Embedded with Wi-Fi or 3G wireless, its users can access their books and buy more books anywhere in the world, where a wireless network is available. M2M has found its way into personal navigation devices, digital picture frames and ereaders already. Sport shoes can be equipped with a short range wireless device that together with a smartphone connects to a website, where progress of a run is followed. Televisions, stereo sets, DVD-players, weather stations, personal game devices, home security systems, all are Internet-enabled these days.

A difficult question for the use of 2G/3G/4G wireless is: how to connect and who pays for it? From a usability, logistical and build quality point of view, consumer electronics companies prefer devices that do not require user interaction, regional solutions or constructions where SIM-cards need to be inserted. They would prefer a solution where the SIM-card is soldered as a chip onto a board, with the same device being sold globally. A consumer electronics company currently would have to sign up with one mobile operator globally to enable this capability. It would spur competition if such a company was somehow able to use the same SIM-card globally, but contract different networks locally. This way a consumer electronics company may be able to get more favourable rates than individual consumers for data connections. A consumer electronics company may also be able to innovate in the way it sells connectivity to its customers. For example, ebook reader service providers receive a payment from the sales of ebooks for the “free” access that consumers have to online ebook stores. A further example could be that a digital camera could come with a prepaid number of pictures that can be uploaded to Facebook, or photo sites like Flickr, and free uploading if sent to a photo printer, where the photo printer pays the cost.

In 2010 some speculation surfaced in media reports that Apple was trying to find ways to embed a SIM-card in a device, in a way that could send the mobile operators credentials via iTunes, or over the air, when the device was activated. Another suggestion was that Apple could become a (data-)MVNO on mobile networks by using SIM-cards. In the following month, the GSM Association announced it would re-evaluate technical possibilities for over-the-air updates, something that it had seemingly not favoured in the past. One of the possibilities a manufacturer like Apple (or its competitors) would have if it was to be an MVNO, is to sell access to mobile networks in a competitive environment. For example, a consumer could choose a wireless access package that fits their wireless data demand, without needing a SIM-card. Or when going abroad use a local mobile operator in that country on a daily package for the duration of the visit, instead of having to get a local subscription, pre-paid card or pay data roaming charges. Another option is to sell music subscriptions to wireless enabled music players, so that users can access a library of millions of songs wherever they are. These innovations in consumer electronics would spur the development of new markets. The final section explores ways authorities can lower barriers for these markets to develop

In late 2010, there were press reports that Apple was working with SIM-card manufacturer Gemalto on SIM-cards that could be updated remotely and the GSM Association announced new work that delivered a proposal for a solution to ETSI, in February 2011. The technical solutions are, however, only partial solutions to the problems of the M2M users. It still keeps the full dependence of the customer on the MNO as a basic principle. It also does not look like there will be a mechanism that allows M2M customers to change subscription frequently and at will, *i.e.* whenever they cross a border or when a network is down. A change in policies and practices may make such requirements possible.

Changing the paradigm by putting the M2M user in charge

An alternative would be to shift the paradigm of mobile communications and to bring the M2M user in control of the SIM-card, authentication, routing and so forth. This was researched for the Dutch Government by Logica.[20] The M2M user would do exactly the same thing as MNOs have done for their M2M subsidiaries. Logica found that this is technically not difficult, though some commentators may disagree. Critics of the Logica view say any potential technical challenges should not be underestimated and that all stakeholders need to be consulted in the development of new approaches. What would be necessary is the equipment to do the authentication and routing of traffic. A third party like a Mobile Network Enabler already provides such services to MVNOs (for instance those operated by supermarkets) in many countries and almost all network equipment vendors have a services department that manages this type of equipment for MNOs.[21] In essence, the M2M user would become, on a technical level, the same as an MVNO on the mobile network or an incoming roaming device and the MNO a connection provider. There are commercial and regulatory consequences to this proposal. On the commercial side it would give M2M users wholesale access to mobile networks. At the regulatory level it would be equivalent to a private network. The implications for regulation will be discussed in the next section.

The benefit it would bring to an M2M-user is that, by being in charge of the SIM, they can determine the parameters of the service they want to use on the mobile network. Some examples:

- National roaming: they would be able to contract two or more MNOs for national roaming. This would give the user improved coverage without the need to have to install two SIM-cards.
- Switch mobile operators: they would be able to switch mobile operators at the end of contracts without having to switch SIM-cards or to contract more or less operators whenever they wished to do so. This could increase competition into the market.
- No international roaming charges: An M2M user would be able to negotiate contracts in multiple countries using the same SIM-card and receiving in each country the rates that are applicable for local use of the network instead of the higher rates for roaming.
- Access to home gateways: An M2M user would be able to negotiate with multiple broadband providers possibilities to use home gateways, instead of just those affiliated with a particular MNO.
- Technical simplicity: It would allow the user to solder the SIM on the communications module (or other technical solutions) instead of using the plastic SIM and a slider.

This type of business model, where the user is in charge, already has precedents. The Netherlands and the United Kingdom both have introduced regulation that allow the DECT-guardband to be used for low power, unlicensed GSM networks, so-called private GSM. It is used, for example in hospitals to address indoor coverage issues and to allow the use of GSM even when the network service of an MNO is temporarily interrupted. The Dutch Department of Defence has it is own Mobile Network Code, that allows it to make its own SIM cards. It has worked on establishing its own GSM network using license free frequencies. It has allowed them to introduce their own GSM networks on sea faring vessels and in military bases in Afghanistan. Press reports suggest Apple is looking at the same type of business model. It is also not unlike the way the Internet works, where end-users take responsibility for their communications and the services they offer and use. For Internet communications the network provider plays a limited but essential role, routing packets regardless of content. This has led to rapid innovation and a thriving ecosystem. Regulators do need to ascertain that where appropriate these private networks meet the legal

obligations that apply to them and on the other hand that existing regulations do not unnecessarily burden private networks.

Increased competition because of M2M users having wholesale access to mobile networks

The effect on the way the market is organised could be quite profound if M2M users could be able to buy wholesale access to mobile networks. The user would have the freedom to organise the set of business relations that allow it to connect to radio networks of mobile operators. It would have the possibility to move from one operator to another or to multiple operators. However, if it was a global player and wanted to offer its services in every nation, it might have to negotiate with up to 800-1000 radio networks and connect to around 190 networks. This would be far from easy and even MNOs have found this to be a burden. For this reason MNOs have established or joined roaming hubs that allow their customers to roam on many networks, with the MNO only needing to connect to one hub instead of a separate connection to each specific network. In principle the M2M-user would have to join such roaming hubs too, to get better coverage quicker.

There may, however, be barriers with M2M-users joining roaming hubs. Research by the European Commission, and comments as part of its consultation on roaming, indicate that it is nigh impossible for MVNOs to get access to roaming agreements. There does not seem to be any specific technical difficulties as MNOs are able to let their M2M MVNOs enter into bilateral and multilateral roaming agreements. There seems to be an issue, or potential problem, with the functioning of the market. Whether or not M2M-users will be blocked from accessing these agreements remains to be seen. On the one hand, it could be argued that a customer willing to pay for access to a network for millions of cars or consumer electronics devices is something an MNO will not say no to. However, MNOs fear commoditisation and see themselves as full service providers and not as just radio access network operators. If MNOs do not break ranks, it will be difficult for an M2M-user to get global coverage. This may be complicated because many arrangements regarding roaming and interconnection are only accessible to GSMA members, which is only open to membership for mobile operators with spectrum licenses.

For M2M users that do not need international coverage it may be easier to convince a single operator to break ranks, especially when there is a large contract to be negotiated. Smart metering contracts totalling hundreds of thousands of meters, may well allow M2M users to negotiate on their own terms. With one or more smart metering deals leveraging open the market, it may well be that other M2M users will be able to follow.

A hybrid market for M2M is a possible solution. If the M2M-users are capable of using the new standards proposed by the GSMA to update their own SIM-cards remotely, they may well be able to have multiple virtual SIMs in the device. The primary being their own, under their control, but for markets that they have not been able to achieve a local roaming deal with, they may be able to fall back on the credentials of an established MNO. It would also allow them to sell parts of their businesses and move the customers to the new owner with a new IMSI.

Some commentators, on the Logica report, have raised the question of whether there is a role for MVNOs or other third parties, where it was not the M2M-user, but the third party managing the SIMs and contracts. They would be in charge of roaming and switching of networks. There may be several problems with this model. For example, the M2M-user is locked in with the third party, where it has no insight in whether the savings the third party makes in contracts are passed on to itself, or what an increase in prices is based upon. This may mean, in fact, that the M2M user was worse off.

Conclusion

For large-scale automobile makers, smart metering initiatives, central governments, and consumer electronics companies and maybe even cities a move towards becoming wholesale customers, may overcome some drawbacks evident with current market structures. The reasons why this has not happened yet are in part because MNOs have not felt compelled by competition or opportunities for growth to offer such services. For some operators it may seem that such a development would mean that they lose control of the customer and are reduced to a radio access network operator. In addition, because such an option is not offered, it may not occur to M2M-users that it is possible. It could be that the notion is a "paradigm shift", for some participants in the market, with smart metering initiatives being at the forefront of acceptance of these ideas. Another important reason why this type of development is not pursued may be because regulators have not made access available to the necessary numbering resources. This could include IMSI-numbers, but also telephone numbers and possible other numbers. This will be discussed in the next section.

THE IMPLICATIONS OF LARGE SCALE M2M USE FOR REGULATORS

The increasing use of M2M could create a range of issues associated with market liberalisation, frequency, numbering, privacy and access to public sector information. Due to the large scale and widespread use of M2M, that is forecast, these issues may have different characteristics than similar debates in the past. For example, concerns around the potential implications for privacy have forestalled or prevented developments in the area of smart metering, until they are addressed. This is somewhat different to other new communication developments, where it is more frequently the case that such concerns arise after a new service is in the market. At the same time, as discussed in the previous section, greater access to the wholesale market, for wireless networks, could redefine liberalisation and number policy. In this section some of the issues that M2M will influence will be outlined. Market liberalisation, in combination with the management of numbering, will be further expanded in a later section and the implications it may have for the consideration of policy and regulation.

Access to (Public Sector) Information

M2M will enable the creation of a wealth of information on all aspects of economies and societies. This data can have different applications, beyond the primary reason it is collected. These data can be used to improve services to users or to create new services and new sources of information for public and private organisations. Some examples mentioned, in this document, are the use of traction control data of automobiles to inform authorities of road conditions (*e.g.* slippery). Another example mentioned is from the Paris Velib network. The system allows users to access the data on where bicycles are available in their vicinity. A third example, not yet mentioned, is how combining the data of 1000s of devices continuously measuring blood sugar levels in diabetics could be used to get more fine grained insight into diabetes. There could be a multitude of other information derived from M2M applications as well. The key question for governments is how to foster an environment where this data is used to enhance welfare.

For M2M data collected by the public sector as part of its various roles, the "OECD Recommendation of the Council for enhanced access and more effective use of public sector information" C(2008)36 is valid. It recommends governments promote openness and for broad non-discriminatory competitive access and transparent conditions for re-use. Whenever the public sector develops M2M projects it should seek to include a mechanism, so that the data can be used in new ways to enhance the value of M2M for the public.

When data are gathered through M2M by private organisations, the case may undoubtedly be different. The data may be valuable to others than the company gathering data, but whether it is available is often up to the private organisation that has made the investment and understandably wishes to maximise its return. Nevertheless, such data may offer welfare enhancing capabilities. One such example is the data gathered by smart meters. The smart meter could be designed in such a way that it shares its measurements with devices in a household. This could allow innovative services, for example a light that changes colour from green to red when energy usage exceeds preset levels, a simple visual way of showing energy usage. In this case the energy supplier may find it in their interest to include this feature, for its customers, or governments, as large customers themselves, may request this service. Governments could encourage research in approaches leading to "win win" outcomes to the sharing of data or consider funding developments that could lead to broader economic and social benefits.

Privacy and security

It is beyond the scope of this report to discuss the full impact of M2M on privacy and security and therefore this paragraph is limited to showing some examples of how M2M impacts privacy and security. Not all M2M services have a privacy component to them, but when there is one, it can give a detailed view of a user's life. With up to 10 devices per person communicating, there will be a significant increase in the range of information potentially gathered on individuals. Health parameters, reading habits, location data, energy use, driving style and eating habits M2M can record it all. All this data can be recorded on individuals and used in a variety of useful applications, but it can also give a confronting insight into the lives of people.

When evaluating the privacy impacts of M2M, it is not enough to look only at the service itself. The network used for the service adds a layer to the privacy evaluation. The registration is, not just a record in the database of the M2M service provider, but equally a data point in a database of a (mobile) network provider and/or in a home gateway or device. The sharing and combining of data, through cloud services, will increase the locations and jurisdictions where personal data resides.

Some implications for privacy issues in relation to using M2M can be indicated through examples:

- A Pay As You Drive insurance monitoring device may log data on the location, time, distance, speed and other parameters that can influence an insurance premium. This can provide a detailed look into the use of the vehicle and the lives of its drivers. Not only does the insurance company store information on a vehicle's users, a range of other firms may do so as well (*e.g.* the telecommunication company). Unlike a mobile phone, the communication module in an automobile will activate itself when the car starts and deactivate itself when the vehicle stops. These are two distinct events that are recorded by the network. Mobile telecommunication companies in the European Union will have to keep a record of the start of every communication under European Union data retention law, every time the car is turned on, a record is made and the start and finish of a trip is known. (article 4.f.1. 2006/24/EC)

- Some M2M services may rely on the aggregation of data shared by thousands or millions of devices. An example could be data on movement of automobiles gathered by providers of navigation devices. This data could be very useful for policy makers or transport authorities who wish to measure the effects of new roads, construction works and so forth. Anonymising these data is, however, not necessarily a simple matter. Researchers have shown that correlating the data with external sources of information and pattern analysis can identify individuals.[22]

- Privacy concerns halted and required a reformulation of the introduction of smart metering in The Netherlands. The standard for the meters stipulated that the data would be recorded and send every 15 minutes, with space for 960 values in the meter (10 days). The 15 minute spacing was chosen to coincide with the interval under which wholesale electricity is bought and sold on a spot market in The Netherlands. The Dutch privacy authorities, however, objected to the potential intrusion in to people's lives.[23] This was because the recording would allow a detailed pattern analysis of people's lives, whereas the main reason why the meters were introduced was for automatic meter reading. The result was a considerable delay and reformulation of the relevant laws, so that the values are collected only several times per year, unless the consumer gives

informed and explicit consent to more frequent meter readings (*i.e.* for energy saving purposes or for smart grid purposes.

Box 6. Smart cities

Though there is not a formal definition of what a "Smart City" entails, the use of M2M features prominently in many examples given of it. The goal of M2M, in a smart city, is to provide citizens and managers of the city, information on and control of the city. Examples are:

- Sensing where traffic is, and adapting traffic lights to it
- Parking spots: sensing if they are occupied and transmitting this information to motorists
- Garbage containers sensing whether they are full
- Green areas in a town equipped with water sensors to regulate irrigation equipment
- LCD street lighting that can adapt intensity when someone walks or drives by.
- Sensors that measure air quality, vibration or noise. The data can be fed into environmental measurements or used to direct police to a disturbance
- Bicycle sharing projects

Sometimes these developments are combined. Street lights can be a platform that hosts cameras, sensors that measure air quality and antennas to receive information via WPAN from sensors embedded in the streets and rubbish bins and relay these onward via fibre or 2G/3G/4G.

Spectrum policy

Wireless M2M devices will influence spectrum policy. Flexible spectrum policies have increasingly become the norm in recent years. These policies attempt to set a minimum of requirements on the application the spectrum is used for and the type of technology that is used. The result being a more liberalised market, where it is easier to move from one type of application or technology to another, if the market so desires. For instance the European Union has changed the so-called GSM-directive in order to allow for technologies like UMTS and LTE to be used in the 900 MHz and 1800 MHz bands, these were previously limited for exclusive use by GSM. Operators are expected to move from GSM to 3G and 4G in the coming decade. M2M will have three implications for spectrum policy:

- It may rigidify spectrum use, because of its expected long lifetime.
- It may lead to alternative uses of spectrum, not always envisaged by the regulator.
- It will likely fill the already full unlicensed frequency bands.

M2M rigidify some of the allocation of spectrum. At this moment, a significant amount of M2M devices are equipped with 2G technologies like GSM and CDMA only. The modules for 2G are inexpensive and effective. 3G has only limited coverage and the high speeds offered may not be necessary. European countries may, for example, see this problem emerge with the eCall system. In some countries automobiles have an expected economic lifespan of 15 years and eCall specifications only call for GSM. Smart meters, by way of contrast, are expected to work for 30 years. Even consumer electronics may be active for 10 years after purchase. The effect of this will be that with an expected lifetime of M2M of 10 to 30 years, the devices will need to continue to work during that period, without needing a replacement of communications modules. This may mean that the customers will want 2G networks to remain active well after 2030. In an industry that, in many countries, is not much older than 15 years, such planning horizons are unusual for some types of communication technologies. This is true for both the industry as well as for

the regulators as the MNO is unable to make commitments beyond the current spectrum licence and governments may not be able to say what their policy will be 5 to 25 years ahead.

Policy makers will need to take into account that the long lifetimes of many government mandated and operated M2M projects, are consistent with the anticipated duration of the technologies that provide their platforms. If mobile operators, for example, desire to shut down 2G networks and government (mandated) M2M devices still make use of 2G, the public purse may be faced with an expensive replacement scenario. Alternatively, there is less choice in the number of available networks for 2G communication if operators decide to shut down their 2G-network. The GSMA's embedded mobile programme has recognised this scenario and commissioned a report, by Analysys Mason, calling attention to the problem and showing that moving to 2G/3G modules has a lower total cost of ownership if forced replacement costs are taken into account.[24]

What further complicates matters is that it is unclear whether choosing 2G/3G modules really is a good strategy. Some analysts, like Analysys Mason, think that some networks will forego the use of 3G in 2G frequency bands. Instead they argue networks will choose 4G technologies, which are both cheaper to implement than 3G and more spectrally efficient.[25] This would mean that if 2G is shut off, those devices using 2G/3G modules will only work in areas where 3G is available, which is significantly more limited than 2G. It is also difficult to evaluate whether 2G/3G modules will be able to switch to 3G technologies in the frequencies used by 2G today. The chipsets, firmware, radio interfaces and filters may only support 3G in the current bands and not in other bands. This has led some analysts to conclude that it is highly unlikely that 2G will be shut down completely and with every new 2G-only M2M device produced, the likelihood of it happening in the near future decreases.

The rigidity of M2M may also impact frequency policies in, to date, less utilised frequency bands, which may in the future be used in alternative manners because of their interesting characteristics for M2M. A clear example is the use of CDMA450 in Europe mobile operators in Portugal and The Netherlands for M2M.[26] Electricity companies in Australia, for example, have also indicated their interest for CDMA450 for smart metering, though they may not have proceeded with it. CDMA450 works in the 450 MHz band and has good characteristics for indoor coverage, much better for instance than GSM900. These bands, in some countries, have been allocated for other uses than M2M communication, but with a more flexible policy, spectrum can be used for M2M. In principle, this type of outcome is what more flexible spectrum policy is intended to accomplish. Other mobile network operators may not have access to this spectrum and may, in the past, not have been interested, because it was not intended or allowed to be used for M2M. This is a relevant point for regulators to consider going forward. The other element worth noting is that these bands can become dedicated for specific M2M applications with a specific technology, resulting in a 30 year or longer claim of these applications on this spectrum. Neither of these two points of concern is negative *per se* as long as policy makers and regulators are aware and accept the implications.

Around the world the most used form of unlicensed spectrum is the 2.4 GHz, which is globally harmonised for unlicensed use. The leading application in this band has been Wi-Fi (IEEE 802.11). In addition, more and more WPAN-technologies are making use of this band. If a greater number of devices interfere with each other, the effect may be that the average performance in the band goes down. This is the paradox of the success of unlicensed spectrum use. Given the complexity of spectrum management and the inherent scarcity it is not a simple matter to provide a solution to this challenge.

Telephone numbers may become scarce

M2M devices require multiple numbers to function on networks. Numbers that many devices will require are:

- IP-addresses (IPv4 and IPv6)
- Telephone numbers (E.164)
- IMSI-Numbers (E.212)

With each of these numbers there is a specific set of issues that will need attention.

The impending depletion of unallocated IPv4 addresses has been expected for some time. This was highlighted in the Seoul Declaration on the Internet Economy and all stakeholders were encouraged to move forward with the introduction of IPv6. At the time of writing, the largest of the five Regional Internet Registries are close to complete allocation of their store of IPv4 addresses. The introduction of M2M, on a large scale, may provide an additional incentive that IPv6 needs to make its adoption more attractive to the market. An IPv4 address is thought to have a market value of roughly USD 10 to USD 40.[27] , A roll out of tens of thousands to millions of M2M devices could lock in hundreds of thousands if not millions of IPv4 addresses. Purchasing these addresses would quickly be considered too costly if the average revenue per unit for the MNO is less than USD 5 per month. Although, at the time of writing, most mobile networks are not IPv6 ready, this is expected to change quickly.

Telephone numbers as defined in ITU recommendation E.164 are another scarce resource that countries may run out of because of M2M. 2G and 3G mobile networks will not work without the use of telephone numbers. This may look a bit odd, because an M2M device is not expected to place a voice call. However when 2G/3G networks were designed, the use for M2M was not a consideration. It is, therefore, not possible to address a device based upon an IPv4/6-address. If the device is operating in a passive mode, without an active IP-session, it will first need to be contacted based on its phone number and activated to set up an IP-session, only then can it be reached. Sending an SMS can only be done with a valid E.164 number. 4G will change this but, as noted previously, 2G and 3G are likely to continue to be used for many years. Furthermore, some countries have as a regulatory requirement that a device has an E.164 number, even when 4G networks will be able to work without such a number. This seems to be an unnecessary restriction.

The Electronic Communications Committee (ECC), within the European Conference of Postal and Telecommunications Administrations (CEPT), has published a report on scarcity of E.164 numbers due to M2M, with a focus to 2020. [28] Based on various assumptions, it was decided to use as an estimate that a country would use 1.4 telephone numbers per inhabitant in 2020. The report concluded that seven of the 29 countries, for which research was undertaken, were expected to face problems with the exhaustion of existing E.164 numbers and another two could face a similar scenario. It is not that countries are expected to fully run out of numbers, but that in the current mobile number range, they will not have enough available numbers. This could require them to open new ranges or to reorganise the numbering plan.

ECC/CEPT evaluated four possible solutions to the scarcity problem:

- Option A: Existing mobile number ranges, including possible expansion of them (E.164 numbers)
- Option B: A new number range for M2M or similar applications (E.164 numbers) (for example longer numbers than normal, however maximum 15 digits according to E.164)
- Option C: An international numbering solution (E.164 numbers)
- Option D: Network internal numbers

Each of these options has advantages and drawbacks and they advise countries to look at national circumstances to make their choices. For example, option B, a 15-digit number range may be difficult to implement and support by network operators with older billing systems.[29] Option D, network internal numbers, does not support number portability or international use of numbers and could therefore not be used for uses that need roaming. The CEPT/ECC suggests to countries that they only give these numbers to MNOs, though it does not set out reasons for this advice.[30] There are a number of potential drawbacks for not making numbers available directly to firms. For example, this could be the case for companies that have an international business and do not know in advance where their devices will be deployed and used. The MNO's of those companies may choose a number range of a particular country, which means that that country will see its numbers used in many countries around the world, but not necessarily in its own.

IMSI-numbers identify individual SIM-numbers. The number is defined in the ITU E.212 recommendation. It is 15 digits long. The first five or six digits are a unique identifier of a mobile network (Mobile Country Code + Mobile Network Code). This leaves one or ten billion numbers for an individual network to assign to mobile phones and devices. For many networks, this seems to be a more than adequate amount. Given that many mobile network operators have E.212 ranges in multiple countries and sometimes even in one country, there does not seem to be an immediate shortage on the level of individual Mobile Network Operators. They would be able to assign between one and 10 billion devices. IMSI numbers are essential to the issue of liberalisation and will be discussed in the following paragraph.

A related problem is that some countries require the use of national IMSI and telephone numbers registered by a national MNO or MVNO for devices that are permanently in the country (and not roaming into the country temporarily). This makes it difficult for large scale M2M users and their service providers to use one range of numbers on a global scale. They would have to adapt each device for a particular market. This can be difficult from a logistics perspective if the SIM-cards in a device cannot be updated remotely; because that would mean the national SIM-card would have to be provisioned in the factory. It is also difficult from a market perspective, because a consumer buying an M2M enabled device from abroad into a country may not be able to access all services or cause M2M users to be in violation of local regulation.

M2M may prompt further liberalisation of the market

In previous sections some indications have been given of the amount of devices that will be connected through M2M and that the M2M-users will want to play a different roll. In many cases they will likely wish to be in control of their devices, determining conditions for national and international roaming and to be able to switch mobile network operators. Being able to undertake this role would be consistent with past reforms to telecommunication markets, that have allowed users to manage their own networks or outsource this function as they deem most meets their requirements. In order for this to be possible M2M-users will have to gain a greater freedom and be able to deploy private networks using public infrastructure. This is comparable to the private infrastructures such as corporate VPN's and Internet interconnections that are currently used by companies and governments over public networks.

Policy makers and regulators would have to introduce changes if the provision of M2M is to be liberalised. The main reason that some M2M users cannot take up their envisioned role, in providing services in ways they deem most efficient for themselves and their customers, is because regulation was established when it was not envisioned that large scale M2M users would need to make use of resources subject to this regulation. Specifically, numbering policy does not allow M2M users access to some types of numbers, that they need to enter the market as direct suppliers of services to themselves or their customers.

E.212 IMSI numbers and some types of E.164 numbers are only available to providers of public telecommunication networks and services. Countries have different specific definitions of who is eligible for these numbers, but in general it can be said that a company will have to offer a network or service to the public in order to be assigned numbers. For example, if an energy company wished to provide M2M capabilities and services to its customers it may not be able to do so, over a direct number assignment made to that company. There are, however, examples of governments that have allowed specific types of E.164 telephone numbers to be used by non-telecom operators, such as social value numbers, emergency numbers and specific company numbers.

Where the distinction lies between the hypothetical energy company and a public telecommunication network provider is very much dependent on the regulatory situation in the country concerned. As a result in different countries companies may or may not already have different opportunities to get access to numbers. In some countries MVNO's do not have access to E.212 numbers, which limits their ability to change network providers and enter into roaming agreements. In some countries a provider of eBook-readers may be able to qualify for numbers, because it provides a public offer of its services. That the eBook device may not support telephony does not, of course, mean that it is not a service that cannot be qualified as a public telecommunication network. The key point in the definition of a public telecommunication network as it is widely applied in relation to regulation, is that the eBook service is available to the general public.

There seems to be very little case law that can act as guidance, though in practice it does seem certain that if a railway company or an energy company wanted to get access to some types of numbers for M2M deployments, it is denied an assignment on the basis that it is using these numbers for private and not for public use. It may use the numbers over public networks, but such use does not constitute public use. The general public cannot, for example, buy a train track monitoring system from the national railway company. Regulatory authorities require private companies to go to providers of public networks for these numbers. The potential outcome could be a lock-in of M2M users, with their network providers, which could limit competition and provide less incentive for operators to act in an efficient manner in meeting customer requirements.

The development of M2M challenges authorities to look into whether the policy to only assign numbers to public providers of telecommunication networks and services still holds. If "private organisations" (*e.g.* private businesses, public utilities) could get access to these numbers and buy wholesale access to networks and enter into roaming agreements, this could lead to a more dynamic market. There are many precedents in telecommunication markets where similar developments have taken place with readily evident benefits for users.

Any organisation can apply for IPv4/IPv6 addresses and Autonomous System Numbers (ASNs) at a Regional Internet Registry, regardless of whether they make a public offer. This allows companies, should they so wish, when they grow in size, to take control of their own routing and interconnections on the Internet. In turn, this enables them to buy capacity for their traffic at wholesale rates instead of retail prices and it allows them to connect to multiple transit providers at the same time, so called multi-homing. If IP-addresses and ASNs had only been available to public providers of electronic communication networks and services, but not to organisations like the BBC, Amazon and Google, or municipalities and banks, they would have to go to an Internet Service Provider and be connected using a range of IP-addresses of the provider and accept the routing of traffic as the provider offered it. Changing providers would result in a renumbering of the internal infrastructure and negotiating global peering and transit based interconnection would be impossible. Today, there are close to 50 000 ASNs in use and this number is still increasing.[31]

For M2M access to E.212 numbers seems most crucial. In a study for the Dutch government, Logica concluded that it was possible to give end-users access to E.212 numbers, without causing problems either

through depletion of the E.212 number range, or by technical difficulties in the networks.[32] E.212 can potentially hold one million independent networks if six digits are used as the identifier of the mobile network (MCC+MNC). However, most countries currently issue five digit MCC+MNC combinations which reduces the potential number to 100 000. The changeover to the use of six digits was not found to be a technical problem as long as it is used in IMSI's used by mobile devices.[33] Issuing MCC+MNC's to private networks for M2M use would also not act as a disadvantage to other policy goals like lawful interception. The report evaluated other solutions such as over-the-air provisioning of E.212 numbers and keys and found that it solved some problems described in this report, but still created a dependency upon operators for (national) roaming and innovation *i.e.* for fixed-mobile convergence.

The fundamental question on the differences between public and private networks and what governments could do in terms of liberalisation of the market could be a topic for future work. Allowing private entities to have access to numbering resources may impact some of the assumptions underlying telecommunication regulation. Relevant authorities would have to evaluate whether existing rules would need to apply to private entities. They would also have to define when an entity crosses from using numbers for private use, to making a public offer of a telecommunications retail service. This is necessary to prevent asymmetric regulation between two entities offering essentially the same service, but one claiming to be a private network and the other being deemed a public network.

NOTES

[1] The work done on RFID was brought together in a document for the Seoul Ministerial. RFID, Radio Frequency Identification, OECD Policy Guidance, A focus on Information Security and Privacy, Applications, Impacts and Country initiatives. *www.oecd.org/dataoecd/19/42/40892347.pdf*

[2] Ericsson presentation at Telco 2.0, London November 2010

[3] Cellular modules for M2M communications related market-research findings in 2010, EETimes, *www.eeherald.com/section/news/nws201102074.html*

[4] *http://media.gm.com/content/product/public/us/en/onstar/news.detail.html/content/Pages/news/us/en/2010/Sept/0909_onstar*

[5] *www.tomtom.com/landing_pages/trafficmanifesto/index-project.php?Lid=1* contains a counter that shows the amount of 2G/3G personal navigation devices. In a phone call, TomTom stated the 20 million target.

[6] TomTom traffic manifesto *www.tomtom.com/landing_pages/trafficmanifesto/index-project.php?Lid=1*

[7] Smart Power outlets presentation at TED *www.ted.com/speakers/john_la_grou.html*

[8] *http://en.wikipedia.org/wiki/HomePlug* The work on this standard is, as of 2010, done in the IEEE1901 working group.

[9] *www.dash7.org/* The Dash 7 alliance

[10] A similar example is the problems consumers have connecting PS3 or Xbox 360 consoles to broadband networks.

[11] For an introduction in the differences between the various generations "2G, 3G, 4G, and everything in between: an Engadget wireless primer", Engadget, *www.engadget.com/2011/01/17/2g-3g-4g-and-everything-in-between-an-engadget-wireless-prim/*

[12] A darkspot is not an unexpected malfunction of the network. The network will work and deliver signal, just not at that particular place and this may be only a couple of square metres. Even though 2G has good coverage in most countries, with often up to 99% coverage of the country. In cities its coverage approaches 100%. However the coverage will have dark spots even in densely populated cities. These are caused by obstructions to and reflections of the signal, so that signal reception will break down. The obstructions can be anything from a truck parked next to a device, a new building built in the area, a reorientation of a cell site or temporary decommissioning of a specific antenna. So called cell site breathing, where the site contracts and expands its size, based on the amount of users/usage may also be a factor. Dark spots on a particular location are often limited to one or two networks and not to all networks, as each network uses different frequencies, antenna sites and network topologies.

13 It is rare for networks to accept any device regardless, to make use of the network. Some people deliberately leave wifi-access points open for anyone who wants to use the network and some wired networks may allow anyone to connect, but this is rare. The same goes for networks that verify only identity based on an address like a MAC-address. Identities are easy to forge. Generally there are forms of security in place to prevent unauthorised use.

14 Some manufacturers of mobile telephones will build devices based on cloned (pirated) hardware and have been known to use only one IMEI. When Pakistan decided to block IMEI numbers of phones reported as stolen, thousands of handsets were blocked after one phone was reported as stolen. The phones had used the same IMEI number, which in turn had been assigned to a reputable manufacturer, but used by a no name manufacturer of mobile devices.

15 *www.slideshare.net/Garry54/simcardsietfppt*

16 Whether or not these business models will be successful is unknown, they are only provided as an example of the types of innovations companies are looking at.

17 Sources: 3GPP's initial thoughts on Machine to Machine Communication, Jorg Swetina, NEC, (*http://docbox.etsi.org/Workshop/2008/2008_06_M2MWORKSHOP/3GPPs_SWETINA_M2MWORKSHOP.pdf).* Communication Diversity Architecture for Smart Networks, Rob Kopmeiners, *http://docbox.etsi.org/Workshop/2010/201010_M2MWORKSHOP/03_SmartEnergy/KOPMEINERS_Alliander_Communication_Diversity_Architecture.pdf* also see 3GPP TR 22.868 en TR 33.812 where it looked at M2M users switching networks in Study Groups 1 and 3, with results published in. The 3GPP identified 4 problem areas for M2M:

- How to prevent stealing of subscriber identity from SIM-card
- How to initially provide the SIM-card with right information either in factory or upon activation in the field
- How to change subscriptions
- How to update the SIM-card to new security levels during a 30 year lifespan

Onderzoek flexibel gebruik MNC' S, Het verlagen van overstapdrempels voor grootschalige M2M gebruikers, Logica, Rudolf van der Berg, Jan Lindoff, 15 juli 2010 . An English management summary is available here: *www.slideshare.net/Raindeer/management-summary-of-onderzoek-flexibel-gebruik-van-mncs* The principal author of the report is the same as the principal author of this document.

18 An example is Amazon's Kindle ebook reader where not all services that are accessible in the United Kingdom or North America are available in other locations, or Ford's SYNC services, which reportedly are seeing problems with mobile roaming (http://connectedplanetonline.com/bss_oss/news/m2m-roaming-put-a-sim-card-in-a-machine-simple-drive-it-across-the-border-difficult-1202/index.html). BMW in a paper on LTE also mentions these problems (www.elektroniknet.de/automotive/technik-know-how/infotainment-und-telematik/article/82391/4/LTE_als_Basis_fuer_innovative_Datendienste_im_Automobil/)

19 Not every mobile network started out with the use of SIM-cards for authentication, though most had a similar function through an embedded chip. UICC's, as the official term for a SIM-card is, are now available in most 2G/3G/4G networks. They can be the traditional plastic slide in variant, but there are also versions that can be soldered onto devices like other chips, which would make them of better use in M2M environments.

20 Onderzoek flexibel gebruik MNC' S, Het verlagen van overstapdrempels voor grootschalige M2M gebruikers, Logica, Rudolf van der Berg, Jan Lindoff, 15 juli 2010 .

[21] Theoretically it is also possible for a company to buy the equipment and manage it themselves. However it is more likely that the M2M user will contract a third party to manage the equipment. This has proven more price effective for MNOs, who have contracted the likes of Ericsson and NokiaSiemens Networks for this and also for several MVNOs who contract Mobile Network Enablers.

[22] For an interesting review of some of the issues involved with anonymising the data of several thousand of drivers in California in a trial by Nokia and UC Berkeley see *http://arstechnica.com/gadgets/news/2011/02/calling-all-cars-measuring-traffic-using-cell-phone-data.ars*

[23] *www.cbpweb.nl/Pages/pb_20080618_slimme_energiemeters.aspx*

[24] *www.analysysmason.com/About-Us/News/Press-releases/3G-embedded-mobile-devices-have-lower-total-cost-of-ownership-than-2G-Analysys-Mason-report/*

[25] *www.analysysmason.com/About-Us/News/Insight/Will-UMTS900-accelerate-GSM-switch-off-in-advanced-mobile-markets/*

[26] Both Zapp of Portugal and KPN in the Netherlands are using CDMA450 for M2M.

[27] Microsoft bought over 666 624 IPv4 addresses from the administrators of Nortel's bankruptcy for 7.5 million dollar.

[28] *www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP153.PDF*

[29] The Netherlands, after consultation with the industry, decided not require all networks to only use 15 digit E.164 numbers per 2012, but to work with a period of flexibility until 2020.

[30] The report mentions the implementation of block routing in networks as a reason. However with the advent of Number Portability and the introduction of intelligent networks and IP-based telephony, telephone numbers do not need to be and generally are not routed based on a block.

[31] Source: Internet Number Resource Report, December 2010, Number Resource Organization

[32] Onderzoek Flexibel Gebruik MNC'S, Het verlagen van overstapdrempels voor grootschalige M2M gebruikers, Logica, Rudolf van der Berg, Jan Lindoff, 15 juli 2010 . An English management summary is available here: *www.slideshare.net/Raindeer/management-summary-of-onderzoek-flexibel-gebruik-van-mncs* The principal author of the report is the same as the principal author of this document

[33] The combination of MCC+MNC as defined by ITU recommendation E.212 is used in two ways in mobile networks. The base stations of the network will broadcast the MCC+MNC to identify the network and it is part of the IMSI that every mobile device in 2G/3G/4G networks has as the basis for identification and authentication in the network.

Some types of 2G networks may not be able to broadcast more than 5 digits to identify themselves, but assigning these networks a 5-digit identifier is not a problem: 10 consecutive 6 digit MCC+MNC's starting from xxxQY0-xxxQY9 is the equivalent of a 5-digit identifier. The mobiles belonging to that network however can have 6 digit MCC+MNC's as the network uses the entire IMSI to communicate with the device and not just the first digits. Some Mobile network enablers have explained that MVNO's may not have their own government issued IMSI ranges, but may have been issued with a range inside the IMSI-range of the MNO whose network they use. The MNO will route all traffic based on the first 8 or 9 digits to the HLR operated by the MNE for the MVNO. It therefore seems technically possible for mobile networks to make use of 3 digit MNCs. The actual use of 6 digit MCC+MNC's will however require

changes in regulations of many countries as most countries currently issue only 5 digit MCC+MNC combinations.