oneM2M

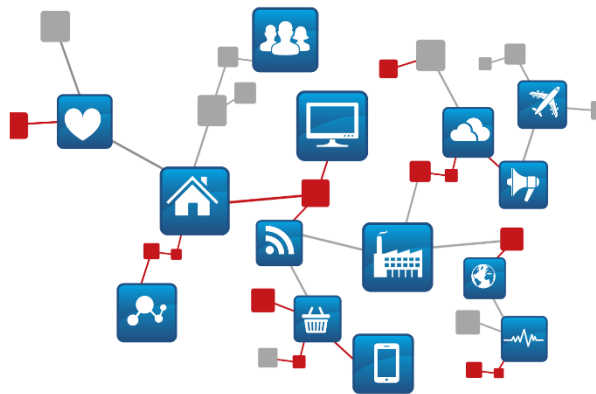## THE INTEROPERABILITY ENABLER FOR THE ENTIRE M2M AND IOT ECOSYSTEM

EXECUTIVE SUMMARY

Market projections for the growth of Machine-to-Machine (M2M) communications and the Internet of Things (IoT) are unrealistic without the emergence of a global standardised platform. This industry will not take off without significant consolidation and the economies of scale that standardisation can bring. Rationalisation needs to occur although disparity will continue on the device and connectivity level.

oneM2M is a set of specifications that will enable users to build platforms, regardless of existing sector or industry solutions. The intention is not to discard or ignore existing industry-specific standards but to work with them to provide value by extending their reach.

For example, a single building or local area solution can be left in place and enhanced with oneM2M specifications that enable wider integration and cross-system value to be derived than is currently possible.

Providing certainty to those investing in new services is critical to the oneM2M concept. Companies need to be sure that what is being built is scalable and robust, and that is a substantial challenge.

oneM2M does not seek to define what organisations will do with the specifications it provides or to prescribe a particular technology or approach. Instead, oneM2M offers a means to interoperate so that all the promises of integration of data and services across and between multiple organisations in different sectors and geographies can be made real.

STRUCTURE

This paper is structured to detail the market dynamics that are requiring greater standardisation as Machine-to-Machine (M2M) and Internet of Things (IoT) markets mature.

Secondly, it explains the need for standardisation and how oneM2M addresses that need as well as areas that oneM2M is not designed to address.

An example of excavators deployed in the global mining industry is provided to illustrate why standardisation is required and what the benefits will be to all the stakeholders in the value chain.
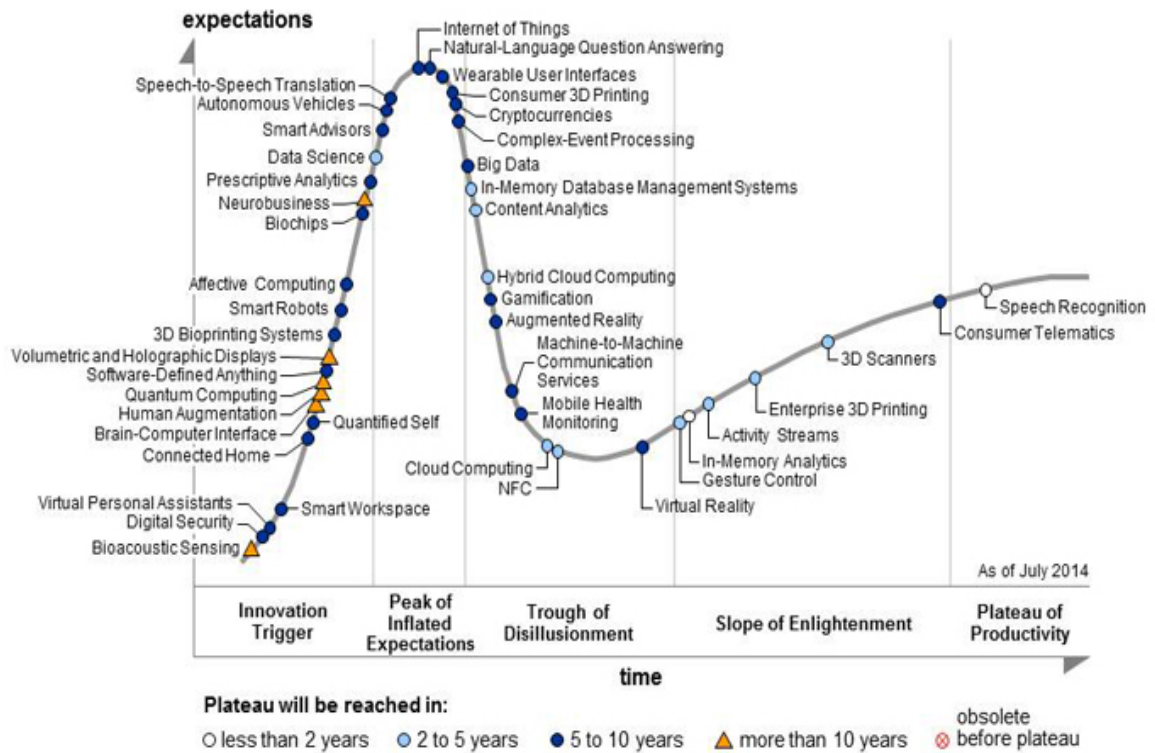
Requirements for interoperability in the network and in data management are examined, as well as the need for consistent security across the Internet of Things to take into account the different security sensitivities of industries and technologies.

1. INTRODUCTION

Most industry analysts acknowledge the Internet of Things and Machine-to-Machine as unprecedented opportunities for creating and commercialising new devices and applications. IoT and M2M will also change the way we live and work through new and innovative services.

There is no doubt that within a few years, there will be a vast increase in the number of connected devices. Analyst firm Gartner places the Internet of Things at the top of its hype cycle for emerging technologies and anticipates a five- to ten-year period for the market to reach full maturity[1].

Figure 1: Hype Cycle for Emerging Technologies, 2014

Source: Gartner, August 2014

Cellular M2M communications will account for at least 10% of the global mobile market by 2020, according to a study by GSMA Intelligence, the research arm of the GSMA[2]. It is forecast that cellular M2M will account for almost one billion (974 million) of the 10 billion total mobile connections expected by 2020 if the market

---

[1] Gartner, Inc.'s "Hype Cycle for Emerging Technologies, 2014."
http://www.gartner.com/newsroom/id/2819918
[2] "Cellular M2M forecasts and assumptions: 2010-2020" GSMA Intelligence, September 2014
http://www.gsma.com/newsroom/press-release/gsma-study-highlights-major-m2m-market-opp/

develops at its current trajectory. Network equipment vendor Ericsson has been projecting more than 50 billion connected devices by 2020 for several years[3].

With a huge base of connected devices, M2M will grow rapidly in terms of revenue. Analyst firm Strategy Analytics forecasts the M2M market to grow at a CAGR of 18%, from $45 billion in 2013 to $242 billion in 2022**.⁴**

The Internet of Things is such a unique phenomenon because it brings together so many previously disparate strands from technology and different industries. The challenge is that there are common requirements for connectivity, security and data handling that cut across all businesses. However, the Internet of Things must also allow for sector specific applications and solutions. Collaboration is therefore not only necessary; it is essential. In fact, convergence of telecoms, IT and consumer electronics, along with software, applications and data handling is required.

Even with such convergence, the main benefit will be easier and cheaper development of siloed applications, by reusing existing infrastructure. Such reuse does not unleash the true benefit of the Internet of Things, where applications can communicate with, cooperate with and reuse one another's data or components.

That is the dream, but the IoT remains several giant steps away from reality. The increasing flow of stories about futuristic IoT applications, such as the connected car or the connected refrigerator, demonstrate that work has been done to create the Internet of Things; however, acceleration is needed to provide the necessary framework for all these machines to integrate and interact with one another efficiently and effectively.

2. KEY DRIVERS FOR MARKET GROWTH

A key driver for accelerating deployment is that most of the technology enablers are in place. Lower hardware costs and wireless data networks are enabling more intelligence and seamless connectivity. Adding a few sensor chips or a wireless connectivity module to a new product or device will not have a notable effect on pricing.

The market is currently able to handle the huge loads of information that all these connected devices will be generating. The availability of big data analytics tools, combined with a growing understanding of how collective data can be used, provides an opportunity to add greater efficiency to M2M and IoT applications.

---

[3] http://www.ericsson.com/oss-bss/blog/heading-towards-50-billion-connections/
[4] Strategy Analytics Machine-to-Machine Strategies (M2) service report, "M2M Revenues by Industry Vertical"
https://www.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5468

Another driver comes from end users. As consumers and businesses have access to, and are used to living and working with smartphones and tablets, they are eager to adopt new applications that enrich the way they live, work, commute or shop.

As the market starts to take off there are growing concerns about the scalability and security of the Internet of Things. However, it is clear that initiatives to standardise architecture, ensure security and enable interoperability are certainly taking the industry forward.

3. WHAT IS oneM2M?

oneM2M is the leading global standardisation body for M2M and the IoT. It was established through an alliance of standards organizations to develop a single horizontal platform for the exchange and sharing of data among all applications. oneM2M is creating a distributed software layer – like an operating system – which is facilitating that unification by providing a framework for interworking with different technologies. Those are the two key elements at the core of oneM2M: providing an interworking framework and enabling re-use of what is already available as much as possible.

The current membership of oneM2M includes seven standards bodies, five global information and communications technology (ICT) fora and more than 200 companies, many of which are in the telecoms and IT industries, but increasingly companies and organisations from other industrial sectors are joining the initiative.

oneM2M traces its roots to initial standardisation work begun in 2008 by the different standards body partners in oneM2M. This encompassed efforts to try to understand what was available in the market and what was missing in terms of facilitators to expand the market and break down the walls between the approaches being taken by different industrial sectors.

It became obvious that there was a need to foster global coordination of these efforts. oneM2M was established to meet the needs of the vendor community to have common solutions that address multiple markets.

The first candidate release of oneM2M specifications was designed to deliver a deployable solution to serve the short-term needs of organisations.

oneM2M sees true promise in combining M2M communications and big data to enable much greater functionality, new applications and mash-ups. The value lies in the insights and benefits created by this combination of data and communications, rather than the communication itself.

4. WHAT oneM2M IS NOT

It certainly is not oneM2M's objective to standardise the whole environment across networks, applications and devices. The objective is to standardise interfaces so they are applicable to the entire ecosystem. The intent is not to limit or excessively specify the activities of individual industries or businesses, but rather to provide a means for them to interoperate openly, but securely, with one another.

5. WHY STANDARDISATION IS NEEDED

Standardisation is needed in order to deliver the scalability and flexibility the market requires to maximise the potential of IoT and M2M. Standardisation enables improved functionality-cost-quality trade-offs to be made, which will deliver faster time-to-market for new devices and applications.

Improving the trade-off is about designing the M2M network for scalability and security. Massive growth in devices, applications, traffic, and profile and usage data must be anticipated now if solutions are to be ready in time to meet the radically heightened demand in coming years.

A standardised architecture with a common set of service layer capabilities and open interfaces and APIs should also help M2M and IoT providers to reduce investments, time-to-market, development and on-boarding costs, and facilitate management of devices and applications. This will help to build a solid M2M and IoT business case that relies on very small revenues per connection, and even smaller margins.

Take the example of smart meters. As many utility service providers want to safeguard their investments for a 20- or 30-year period, network interfaces will have to be stable and device software will have to be manageable and upgradeable.

Standardisation will make it easier for individual stakeholders to partner and interwork with component providers, application developers, solution integrators, data and content owners, and with wireless and wireline connectivity providers.

Providing a unique experience will be key for making the Internet of Things a success -- but many challenges exist. In order to achieve the "any app, any device, any network" objective, devices and applications need to be abstracted from the underlying access networks and technologies. This model can only work when there is maximum interoperability between devices, platforms, data formats, protocols and applications.

As some devices may be deeply embedded in third party infrastructure – such as machines, containers and cars – and may have no registered owner at all, remote management capabilities become extremely important. Many M2M and IoT devices will also be characterised by very small power, memory and processor
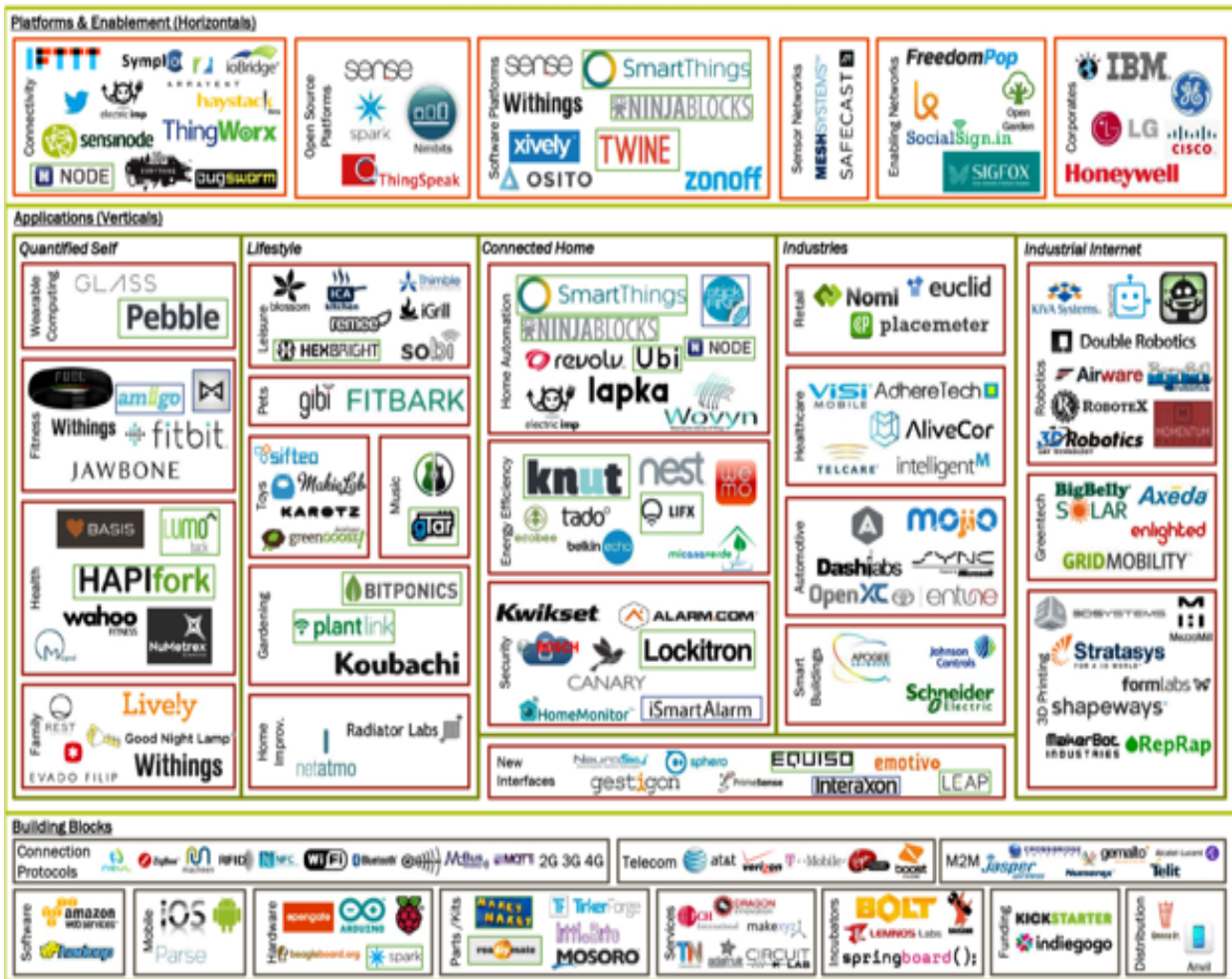
footprints. Therefore, communication and management protocols will have to be simple and lightweight. In addition, security and privacy concerns will need to be addressed and standardisation efforts should encompass authentication, authorisation, encryption and data protection.

6. HOW oneM2M ADDRESSES STANDARDISATION NEEDS

The main reason for the creation of oneM2M is that the entire M2M and IoT market was being held back by an absence of established standards that enable interoperability among devices, applications, data collection and storage across geographies and across industry sectors.

However, as of this writing, little movement is being seen along M2M's projected exponential growth curve and opportunities are not being realized yet. Initially, it was recognized that much of the technology was already available or in development, and many industrial sectors were using long-standing technologies. For example, some technology used in industrial building automation today originates from the 1980s. The fragmentation of this technology landscape creates challenges for M2M and IoT market growth. Even recent standardization initiatives tend to have limited following and risk becoming silos. The emerging need for interoperability across different industries and applications has necessitated a move away from an industry-specific approach to one that involves a common platform bringing together connected cars, healthcare, smart meters, emergency services, local authority services and the many other stakeholders in the ecosystem.

Figure 2: A Fragmented Ecosystem

Source: Matt Turk, Sutian Dong, FirstMark Capital, 2013

oneM2M exists to enable all of these disparate technologies to talk to one another in a single framework.

7. EXAMPLE: DEMONSTRATING THE VALUE OF oneM2M SPECIFICATIONS

Take the example of excavation equipment in the mining industry, an industry with a huge footprint across the globe of heavy industrial plant and site equipment in different locations. A mining company may run excavators made by Caterpillar, JCB, Volvo and Doosan; each may have M2M capability embedded by the manufacturer. The technologies and equipment may be aging, in some cases up to 20 years old. M2M capabilities may have largely been deployed to assist the manufacturer and focus on functions such as preventative maintenance, vehicle tracking and monitoring the number of hours the equipment has worked for. The data and information is fed back to the manufacturer to aid its design of new

products, to help it set prices for leasing of equipment, and to understand the different loads put on vehicles performing specific tasks or working in specific terrains and climates.

Much of the data would be of great value to the mining company. Knowing, for example, that at a mine in Chile a machine needs to run longer to shift the same yardage of material than is required at a mine in Siberia would be useful. Another example might involve the same type of excavator requiring a new part more rapidly at the site in Siberia than is required in Chile.

The challenge involved in extracting all of this data is that each excavator is likely to have a proprietary system that typically communicates back to its manufacturer; the data collected from a Caterpillar excavator will be collected in a different way and in a different format from a Doosan excavator or a JCB. The lack of standardisation radically increases the complexity involved in trying to correlate the data from such disparate sources and extract valuable insights from it.

Data security also needs to be considered. The heritage of the excavator industry is that the manufacturer receives data from the machines and may share it with customers to enable preventative maintenance. However, mining companies may want to share only some of the data an excavator collects and they will be particularly cautious about sharing productivity-related data with an outside organisation.

An independent service provider might be the answer provided it is trusted by both the mining company and the excavator manufacturer to share only relevant data with each party.

An interworking framework like oneM2M holds the promise of enabling a system in a Doosan excavator, managed by a specialist provider, to integrate with the systems of Doosan and the mining company. The value each company gains from the insights can be enormous. For the mining company, it encompasses data on productivity, which machines work best in which situations, which machines are most effective and which are most durable.

For the excavator manufacturer, the data encompasses performance insights, data on the workload of machines, data than can suggest how to enhance and develop their products better and data to help keep their customers happy by providing upgrades and timely preventative maintenance.
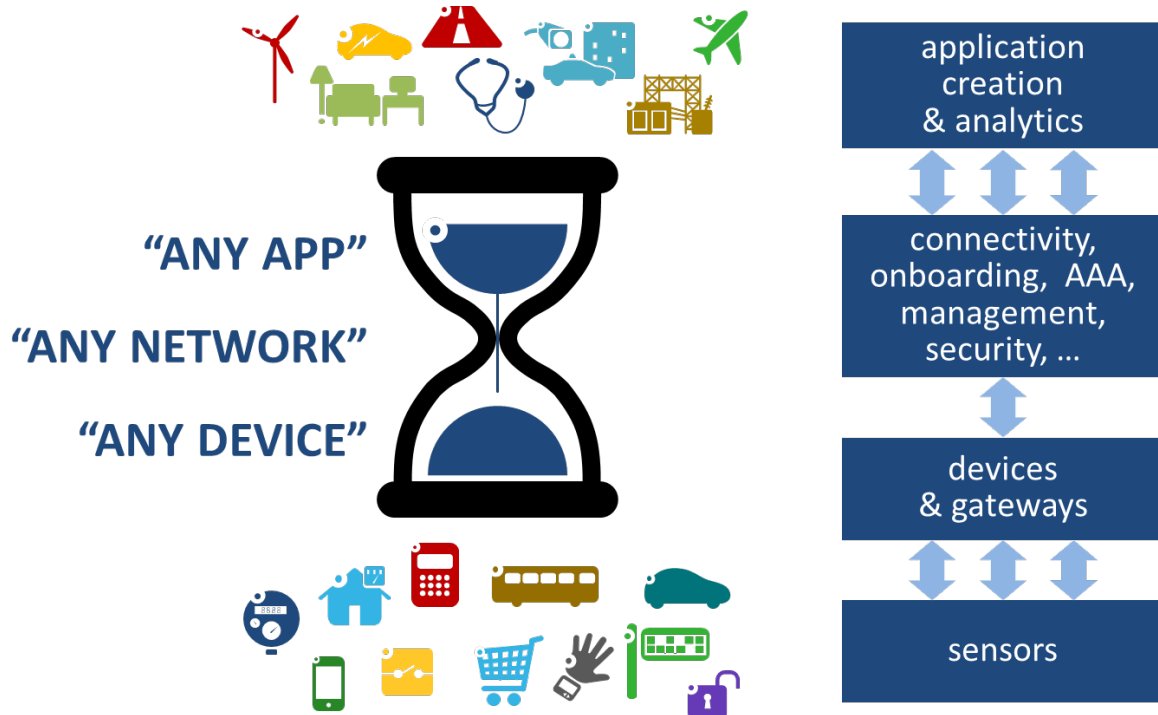
8. INTEROPERABILITY ACROSS NETWORKS

A huge amount of work has already been done to ensure different network technologies are able to support M2M and IoT services. Network interoperability is not the mission of oneM2M.

A lot of technology solutions claim to be network-agnostic but oneM2M proposes that a more accurate description for its capabilities is network-independent. The

difference is that network independence involves knowledge and awareness of the network being utilised to ensure the best service or experience is created. Being network-agnostic means the solution will work regardless of network but it does not mean it will work well, or that the solution can be optimised to reflect what type of network is being used.
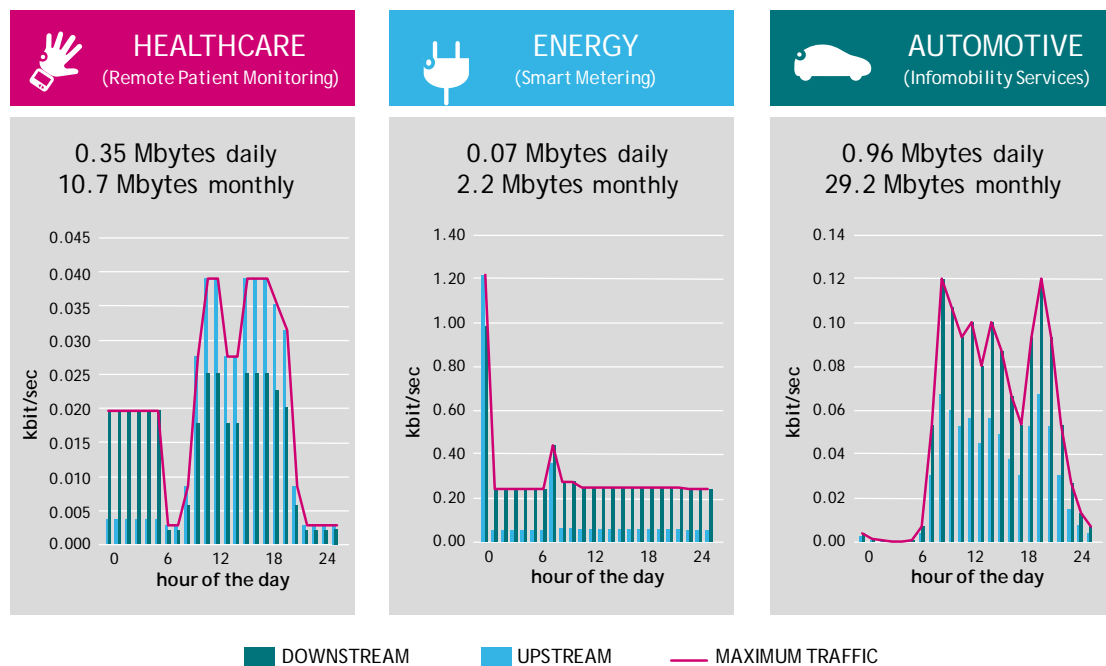
Figure 3: M2M End-to-End Network View

Source: Alcatel_Lucent

The network is the critical enabler and many millions of data points, devices, and apps will generate a multiple of – mainly – very small messages that will flow across networks. Signalling traffic may actually be a primary bottleneck for M2M communications. Modelling by Alcatel-Lucent Bell Labs has shown that up to 67% of computing resources in the radio network controller of a mobile network may be consumed by M2M and IoT applications[5]. Access channel capacity does not appear to pose a problem, nor does data volume.

Sensor-to-application data will far outweigh the control and management information from application-to-sensor but, at times, there will be significant throughput in the latter direction. In the sensor-to-app direction, the traffic may be very application specific – sometimes the flow will be continuous and sometimes it will be in bursts.

---

[5] *Alcatel-Lucent Bell Labs*, Cellular *M2M* Traffic Analysis, 2010

Figure 4: M2M Traffic Patterns for Different Applications

Source: Alcatel_Lucent Bell Labs

9. DEVICE MANAGEMENT

The adoption of device management and service automation capabilities will help the M2M and IoT industry accelerate on-boarding and reduce operating costs. These capabilities streamline tasks such as remote device activation and bootstrapping, device configuration, troubleshooting, firmware upgrades and application lifecycle management.

The shape of the hourglass in Figure 3 symbolises the need for a horizontal M2M control and management platform that allows abstraction of devices and applications from the underlying access networks and technologies. Device management solutions and standards already exist and are in use by different industries. oneM2M takes these standards and integrates them into its solution, making use of what already exists, rather than reinventing the wheel.

10. INTEROPERABILITY OF DATA

One of the greatest value creators that oneM2M can enable beyond smooth interoperability is the integration of data between multiple devices, applications, networks and industries. oneM2M is developing a unified interface for the abstraction and semantics of these data. oneM2M has identified that specific work needs to be done to address the management aspect of specific devices and is developing a unified framework and unified interfaces with high agility to achieve this.

The aim is to abstract data heterogeneously and provide common tools. Work on the data connection and processing part has already begun and a study is ongoing on how to interwork with networks such as Zigbee.

Beyond that, oneM2M is exploring the new area of data semantics to enhance data interoperability. In Release 1 it has introduced a semantics add-on that can discover the attributes of a platform with the names and locations of resources. This is set to improve data interoperability with semantics exchanged in meaningful ways, which will start to truly unlock the value of the data held in all the various systems and sensors across the Internet of Things.

11. ADDRESSING SECURITY CONCERNS

When it comes to ensuring security, oneM2M is working to ensure the needs of multiple stakeholders are addressed. That's a challenge because each type of organisation has different needs and priorities. Each has different security interests. For a telecoms operator security is about ensuring availability, for a customer organisation, it's about protecting their data and for an M2M and IoT provider it's about ensuring uptime.

There is a complex spread of variables that need to be taken into account. For instance, an enterprise might want to use a platform to share certain data with a customer but not with suppliers. For that reason, since its inception, oneM2M has tried to go beyond addressing the needs of one stakeholder and instead focuses on creating platforms that address the whole market's current and future stakeholders.

There's an education battle to be fought because companies deploying M2M and IoT apps, such as mining or energy companies, are not necessarily very familiar with IT security. They recognise that they have to perform risk assessment but they are not familiar with the solutions they can use.

A key challenge to address is how to deploy security credentials to a device in an insecure location to enable it to communicate securely. Security relies on the ability to keep a secret. Credentials need not only to be deployed securely, but also protected inside a device. The huge diversity of M2M and IoT device types, their different capabilities and the range of deployment scenarios makes security a unique challenge for the M2M and IoT industry.

12. CONCLUSION

The Machine-to-Machine (M2M) and Internet of Things (IoT) markets are expected to see significant growth in the coming years. Yet in order to meet and exceed growth projections, the fragmented and expansive M2M and IoT ecosystem will continue to need standards to act as a glue between all the disparate stakeholders. Existing technologies and industry standards need to be linked to enable the complete ecosystem to become more integrated and open.

An umbrella standardisation of this type is vital to enable interoperability in a cost-effective way that also addresses the fundamental requirement for M2M and IoT experiences to be good.

Sector-specific standardisation is a blind alley because all it will achieve is a series of siloed standards between which integration is far from guaranteed. That's not say a degree of intra-industry standardisation isn't desirable and, in many cases, that already exists. What's more important, though, is that a means is provided to integrate with the standards created by other industry sectors.

oneM2M has been set up to create a platform for interoperability to bring the entire M2M and IoT ecosystem together.

It's a simply described concept but far harder to achieve in reality. Today, much of the heavy lifting has been done in terms of specifying how oneM2M will work and how it will be relevant to all organisations in the value chain. It's time for the entire ecosystem to join the project.

ABOUT oneM2M

oneM2M is a global organization creating a scalable and interoperable standard for communications of devices and services used in M2M applications and the Internet of Things.

Formed in 2012 by seven of the world's preeminent standards development organizations, oneM2M membership today consists of thought leaders from a broad range of industries, including industrial manufacturers and suppliers, consumer device manufacturers, component suppliers, and telecommunications service providers.

oneM2M Partner standards development organizations are: ARIB (Japan), ATIS (U.S.), CCSA (China), ETSI (Europe), TIA (U.S.), TTA (Korea), and TTC (Japan). Additional partners contributing to the oneM2M work include: the BBF (Broadband Forum), Continua, HGI (Home Gateway Initiative), the New Generation M2M Consortium - Japan, and OMA (Open Mobile Alliance).

oneM2M specifications provide a framework to support applications and services such as the smart grid, connected car, home automation, public safety, and health. oneM2M actively encourages industry associations and forums with specific application requirements to participate in oneM2M, in order to ensure that the solutions developed support their specific needs. For more information, including how to join and participate in oneM2M, see: www.onem2m.org.