IoT race is a Marathon, not a Sprint …

…the industry needs to urgently increase collaboration: Dr Omar Elloumi, Chair of oneM2M Technical Plenary, and IoT Standards Strategy Leader, Nokia Bell Labs and CTO Group

Dr Omar Elloumi, Chair of oneM2M Technical Plenary, and IoT Standards Strategy Leader, Nokia Bell Labs and CTO Group

Dr. Omar Elloumi is IoT Standards Strategy Leader in Nokia Bell Labs and CTO Group. He is the elected chair of oneM2M Technical Plenary after having led the oneM2M Architecture group delivering the first release of specifications. Omar joined Alcatel-Lucent in 1999 and held several positions including research, strategy and system architecture. He holds a Ph. D. degree in computer science and served on the ATM Forum and IPSphere Forum Board of Directors. Omar Elloumi is coeditor of books on M2M communications and Internet of Things published in 2012. He is also involved in program committees of several international conferences on M2M and IoT.

When it comes to the Internet of Things (IoT) there is one thing we can be sure of – the number of online products and consumer goods will increase exponentially as 2016 continues.

According to Gartner Inc. forecasts, the number of new 'things' which will get connected every day in 2016 is 5.5 million – bringing the total number of connected things in use worldwide to 6.4 billion by the end of 2016, a 30 percent increase from 2015. By 2020, Gartner predicts that figure will reach 20.8 billion.

In this brave new digital world, we will no longer flick a switch to boil a kettle but send it a text message, most probably over the Internet and our homes will, in theory, be more secure, efficient and synchronised. But with so many products arriving on the market, are we getting ahead of ourselves?

Unlocking IoT's full potential
For IoT to truly benefit consumers' lives and reach its full potential, service providers and vendors alike need to look at it as a customer-centric opportunity while remaining focused on the bigger picture. Without this, IoT growth will be stunted and the market will become heavily fragmented, leading to security issues and vendor lock-in.

In this scenario, the IoT dream will quickly become a nightmare for consumers, with the worst case scenario producing a segregated smart home where products can only communicate with other devices of the same brand

▶

► leading to overly complex and time-consuming operations. In turn, this could lead to one or two brands dominating the market, giving them the ability to exploit consumers by charging higher prices as a result of the lack of choice. Other disadvantages this could lead to include less urgency to come up with innovative products to stay ahead of competition, complacency and less choice in the range of products available, hindering the overall progress of the IoT ecosystem.

The 2015 McKinsey report '*Unlocking the potential of the Internet of Things*' shows just how much potential of the Internet of Things could be lost without carefully considering interoperability, stating that interoperability will unlock 40 per cent of IoT revenue.

Pressing the pause button

This reinforces the importance of detailed and well-documented specifications in the IoT industry. While the time required to create globally harmonized standards can create frustration for many of us, this is nothing compared to the frustration consumers and industries will experience if their newly installed IoT system requires multiple controls for multiple devices and actually complicates their lifestyle or operations rather than simplifying them.

Consequently, vendors rushing to be the first to release new IoT gadgets and ecosystems urgently need to increase collaboration and treat the IoT race as a marathon, rather than a sprint.

With this approach, the major obstacles that currently exist in the IoT industry can be overcome. Security, for example, is still a huge issue in the industry, with a survey of more than 6,000 UK consumers conducted by security firm BullGuard earlier this year revealing that 72 per cent of respondents do not know how to secure their IoT devices. Security functions cover identification, authentication, authorisation, security association, sensitive data handling and administration, and have a large variety of deployment scenarios to take into account, involving any type of device, meaning multiple modular authentication and provisioning options, as well as cost-optimized security according to operational requirements.

Delivering on the promise

The good news is that work to produce the detailed specifications required is already underway. oneM2M – the global standards initiative that covers requirements, architecture, API specifications, security solutions and interoperability for Machine-to-Machine and IoT technologies – has developed and is continuing to work on globally recognized technical specifications which tackle the need for a common IoT Service Layer that can be readily embedded within various hardware.

Most recently, we have released an updated edition of our Release 1 global specifications, a development that promises to enable IoT interworking and create a foundation

platform to interconnect IoT devices and applications. The updated specifications, released just one year after initial publication, have incorporated improvements based on early implementation experience and feedback from oneM2M's first Interop event held last year. Requirements, architecture, application programming interface (API) specifications, security solutions and mapping to common industry protocols such as CoAP, MQTT and HTTP are all covered in the technical documents.

By building upon well-proven protocols that allow applications across industry segments to communicate with each other, the updated standard enables service providers to combine different IoT devices, technologies and applications – a critical feature in their efforts to provide services across a range of industries. Release 1 has already been used in service provider deployments in South Korea, Asia and Europe for smart city and transport system deployments. Most importantly, the updated standard presents the industry with the first scalable and future-proof platform upon which it can invest and develop IoT applications, without fear of vendor lock-in or needing to commit to one connectivity technology.

The oneM2M global alliance is now working on the second release of its specifications, which it expects to complete by mid-2016. The updated standard will include enhanced security, features for home domain and industrial domain deployment, semantic interoperability, and interworking with popular IoT device ecosystems such as AllSeen Alliance, OCF and OMA LWM2M. These features will present the unique value proposition that application developers have been looking for – one common core interworking platform technology for the Internet of Things.

Conclusion

As we move forward, it is important for service providers and vendors to remember the IoT is still a nascent market. The ability to spin up a new solution can be quite daunting; there is a lot of effort involved in integrating a complete solution especially if you have to deal with legacy systems; this is the case for smart cities in particular. With standards-based solutions, customers are given access to an eco-system of multiple solution providers. This is the only way to ensure multi-vendor interoperability and supplier choice and, therefore, deliver on the actual promise of IoT.

For more information visit:
www.onem2m.org