

White Paper

“Lightweight M2M”: Enabling Device Management and Applications for the Internet of Things

Guenter Klas, Vodafone
Friedhelm Rodermund, Vodafone
Zach Shelby, ARM
Sandeep Akhouri, Ericsson
Jan Höller, Ericsson

Feb 26th, 2014



Executive Summary

This white paper gives an introduction to a new, emerging communication standard with high relevance for the growing machine-to-machine (M2M) industry and the Internet of Things (IoT) as a whole. In short, this open industry standard provides a means to remotely perform management of a wide range of remote embedded devices and connected appliances in the emerging Internet of Things, to perform remote service enablement and remote application management.

The market for connected devices is growing tremendously. Though there are industry standards available that cater for the remote management requirements of e.g. fixed network broadband routers and smartphones, those established standards are not particularly useful for the remote management of a large and growing category of connected devices: those with limited network bandwidth, computing power and memory, those depending on a limited battery lifetime and those viable only at very low production costs. Hence, this new effort was undertaken to create a mechanism that also caters to the needs of ‘constrained’ devices. The industry has been looking for a simple, low-cost remote management and service enablement mechanism, which embraces modern architectural principles (in line with Internet standards), also works over wireless connections and is fit for purpose due to being lightweight. This new standard is thus called OMA Lightweight M2M (LWM2M).

Technically, it is a communication protocol for use between client software on a M2M device and server software on a M2M management and service enablement platform. The LWM2M protocol, to be used for remote management of M2M devices and related service enablement, has at least four outstanding characteristics: 1) it features a modern architectural design based on REST appealing to software developers, 2) it defines a resource and data model that is extensible, 3) it has been designed with performance and the constraints of M2M devices in mind, and 4) it reuses and builds on an efficient secure data transfer standard called the Constrained Application Protocol (CoAP) that has been standardised by the Internet Engineering Taskforce (IETF) as a variation of the Internet’s HTTP protocol (appropriate for data transfer to and from low-cost connected IoT devices).

This new client-server protocol has been specified by a group of experts in a standards project of the Open Mobile Alliance (OMA) and is based on protocol and security standards from the IETF. As an OMA industry standard, the related specification is freely available. The new LWM2M specification has recently been ratified by the OMA. Various companies have already implemented the standard and performed initial interoperability testing. Implementations range from prototypes and demonstrators to commercially available software clients for M2M devices, hubs, gateways and M2M service platforms.

The availability of this open, standardised remote management mechanism creates the following opportunities and business benefits as applicable for various players in the M2M industry:

- It will reduce the degree of fragmentation in the area of remote management for M2M, thereby enabling more plug-and-play solutions between an increasing variety of M2M devices and the M2M service enablement and application management platforms.
- Given its design to additionally cater to constrained devices, it can act as an enabler to grow the M2M market in various segments ranging from Smart City management, energy management to location tracking. In particular, it will benefit domains where the remotely controlled M2M appliances need to be of very low cost to enable sustainable business models.
- As the core communication mechanisms are working with an extensible data model, the use of LWM2M can be expanded into market areas that turn out to benefit the most from its design characteristics.
- This new standard will greatly improve time-to-market and the manageability of devices, for the first time providing a solution that can be used for both device management and application data and services regardless of how the system components are hosted.
- As an open interface remote management protocol standard between M2M appliances and server-side M2M platforms (optionally Cloud-based), it leads to a decoupling of both sides, thereby enabling greater independent innovation of M2M devices and M2M platforms.
- Growing number of M2M connected devices enable economies of scale, thereby providing more choice for M2M customers regarding M2M devices and their management platforms, less vendor lock-in and hopefully greater viability of M2M solution deployments.

1. Introduction

In this white paper we provide an overview of what an expert community has named OMA Lightweight M2M (LWM2M). At its core is a new, technical industry standard for a communication mechanism between M2M devices and M2M service platforms. Already today, millions of devices around the world are deployed, controlling industrial machines, street lights, or reporting sensor data as useful for smart city management or eHealth applications.

In Section 2, we will look at the key motivations for creating a new technical standard for use in M2M. To this end, we consider the current situation and highlight the issues the industry faces. Section 3 will provide an introductory understanding of the new mechanism and protocol specification called LWM2M. In Section 4 we then look at the opportunities and benefits, commercial and otherwise. In Section 5 we compare LWM2M with the well-established OMA DM standard. Finally in Section 6, we take a step back and consider the wider ecosystem, and how it can benefit from this new industry specification.

2. Market Motivation

2.1. Device Management and Applications

Machine-to-Machine is and will stay a growing area. According to Analysys Mason, the number of wireless M2M device connections will grow from 200+ million at the end of 2013 to 2.2 billion in 2023 [1]. Analysts in general are predicting that the Internet of Things will have over 20 billion devices as of 2020.

The M2M industry is comprised of different segments such as automotive, smart city, building automation, smart energy, manufacturing, agriculture, security and safety, health, education etc. Although the use cases are quite different, all these areas have in common that they require not only connected devices able to communicate over a variety of network connections, but these devices also require remote configuration and control capabilities. For example, M2M devices may need to be remotely 'woken up', they will require several firmware updates during their lifetime, or devices need to be configured for a certain network bearer, or data reporting periods and measurement thresholds need be set, or the device's location has to be provided to a tracking centre. There is unlimited potential for real business benefits to companies in these industry sectors. It is commonly recognized that the millions of connected devices that make up M2M systems and are part of the Internet of Things need to be switched on, configured, provisioned for services, maintained, updated with software, possibly switched off and on again, recovered from error conditions, monitored, queried for data, repaired, their applications managed and finally the devices taken off their network connections at the end of their lifetime. And ideally, all this happens remotely. This is the need for device management and application management, for which LWM2M provides a solution.

The range of use cases and the functionality required to enable them are very broad. A plethora of devices and solutions are available for customers, however, a large amount of the employed technology is proprietary today. This entails drawbacks for customers as far as vendor lock-in and relatively high costs. Today the picture of the M2M market is one of a highly fragmented landscape with margins that could be much better. The market indeed makes use of a few industry standards but most of those are limited and suitable only for a specific market segment. In particular there has been a lack of a mechanism catering to the needs of the next billion connected devices entering the market place: e.g. smart appliances that become Internet connected, play a major role in overall end-to-end applications, need to be of very low cost and may have other constraints (like a single battery lifetime, or limited processing capability due to physical design constraints). LWM2M has been designed in particular to manage the lower-cost, more constrained devices (like a battery-powered location tracker attached to a container box or a streetlight controller). However, LWM2M is also able to manage more high-end capable M2M devices (like an industrial hub or gateway).

In particular when it comes to performance- and cost-constrained M2M devices, standardised device management mechanisms as they are available today from adjacent areas (e.g. broadband DSL router management or smartphone device management) are not the first choice as mostly over-engineered and inefficient. That's what inspired the designers to call the new client-server management standard Lightweight M2M.

It is also obvious that the lack of industry standards in certain areas is hindering the growth of the M2M market. We are focusing here in particular on the question of how M2M devices and their applications can be remotely managed. Do M2M devices come with their own bespoke remote

management solutions? Or is there a choice to be had? Can customers select or even design themselves the most suitable device and then independently answer the question how (through which software system, or which party) to remotely manage the device? The current degree of fragmentation leads to longer solution development time (e.g. when you select a device that comes either with inadequate or no remote management capability), higher costs for M2M customers due to vendor lock-in and lack of economies of scale and barriers to innovation.

Thus, as a more general rule, introducing some standardised interfaces helps to decouple system components, leads to plug-and-play, unlocks innovation in individual system components, increases competition and enriches the market place with products suitable for many more customers.

Members of the Open Mobile Alliance have identified the need for an application layer standard for device management and service enablement, which can be used across various industry segments. This has led to the development of a highly innovative, slim and efficient client-server protocol with a data model, which can be extended to support almost any kind of use case. It is the vision of the companies, which have developed OMA Lightweight M2M that this new Enabler will support the creation of an Internet of Things based on interoperable standards, such as the success of today's Internet would not be imaginable without standards.

2.2. Moving Past Vertical Silos

In the previous section we laid out the motivation for LWM2M by arguing there is a need i) to overcome the issues from technical fragmentation, ii) to find a suitable mechanism to cater to the needs of constrained M2M devices and iii) to generate benefits from decoupling system components via standardised interfaces. Let's introduce some further arguments here.

As often is the case in new and growing markets, everybody sets out to grab land and try to make money. In that early stage of an industry early adopters are keen to get solutions and many good solutions are created. First as pieces of a puzzle (e.g. M2M devices only), then as more coherent end-to-end solutions (e.g. manageable devices and applications). The market then grows, success attracts more players, margins tend to shrink, the types of customers become more varied, economies of scale become important and business models get adjusted. Today's landscape is partly characterised by stove-pipe solutions or vendor-proprietary vertically integrated solutions (e.g. you may get M2M hardware, device management and application management from a single source). Though that's exactly as it happens when a new kind of industry emerges, it doesn't tend to be a sustainable model in the long run as it leads to high costs for the customers in the industry and a lack of interoperability across vendors. Though it of course allows a particular party who offers a vertically integrated solution to innovate along their own product/service roadmap, it stifles innovation in a broader sense, as new innovations e.g. on the M2M device and client side are not able to 'plug-and-play' together with independent new innovations on the server side. Decoupled systems and open or standardised interfaces are the answer to this issue.

Open interfaces between the M2M device/client side and the M2M service platform side have benefits for many parties in the value chain. To state a few:

- M2M device and appliance vendors don't have to worry about finding a suitable mechanism to get their equipment remotely managed. Given an open interface, parties with skills and core competence in remote management will offer those endpoints.
- M2M platform operators and service enablement companies can optimize their costs due to being able to reach many more new M2M devices through a common open interface. This avoids repetitive implementation of bespoke, vendor-proprietary or customised protocol endpoints on their systems. This is expected to translate into benefits for M2M customers.
- M2M application and equipment developers will embrace an open off-the-shelf standard that enables them to get their products remotely managed and connected to any M2M management platform that implements that open interface. An open, standardised management interface like LWM2M, once adopted by a wider community should provide particular benefits for M2M developer communities in terms of available documentation, tools, reference designs and the like, accelerating time to market.

The expert group that has designed the LWM2M standard in OMA was not the only group to appreciate the need for more open standards in the M2M arena. Starting in 2010, work was initiated in ETSI on a more comprehensive M2M architecture, embracing the notion of open interfaces right from the start. This work was partially transferred to oneM2M in 2012 to broaden the participation of companies beyond Europe. In essence, the OMA group on LWM2M has produced a client-server protocol specification that fits into the overall M2M architecture of oneM2M. Similarly, the needs of the M2M market have been on the agenda of IETF for a long time. The results of work already completed by IETF to create an 'HTTP-like protocol suitable for constrained devices', called CoAP along with standard REST interface designs have been used as the basis for LWM2M. The group thereby acknowledged the usefulness of previous standardisation results and layered protocol architectures, the need for a modern system architecture¹ and the desire of the industry for quick results.

¹ Leaning towards REST architectural principles and leaving behind the legacy mechanisms of SyncML.

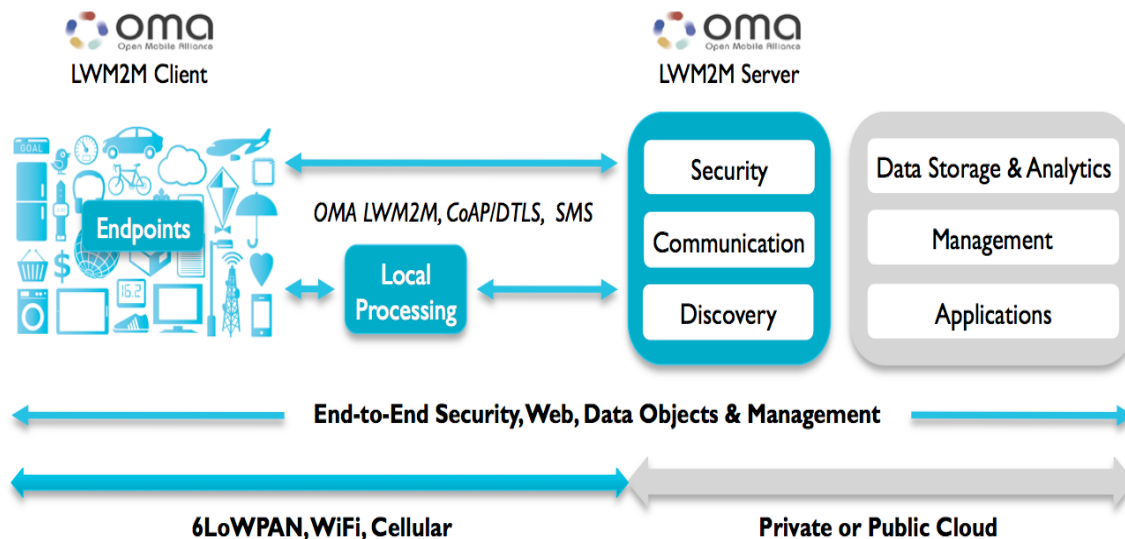


Figure 1 LWM2M deployment scenario

2.3. Access to Constrained Devices over Low-Power Networks

The M2M market has traditionally thought of itself as providing access and management to Cellular based devices and gateways. Home and building based systems using non-IP based local networks such as ZigBee Pro or Z-Wave have used a similar model, providing access and management of a gateway device. Over the past 5 years technology for low-power local communication has changed radically, with a trend towards end-to-end communication with the Internet. The IPv6 over Low Power Wireless (6LoWPAN) standard from the IETF now enables IP communication over any low-power wireless or even wired (e.g. PLC) medium. We now have standards for 6LoWPAN over IEEE 802.15.4 (the ZigBee IP standard), 6LoWPAN over IEEE 802.15.4g (the ZigBee NAN standard), BT Smart and PLC communications. These networks are typically designed for payloads under 127 bytes. Devices typically have limited Flash and RAM (e.g. 16 kB of RAM and 128 kB of Flash) and often limited power budgets.

The fact that these standards now allow any low-power device to communicate with back-end systems directly or indirectly using Internet standards changes the model for M2M. Together with lightweight communication technologies provided by Lightweight M2M, advances in low-power 32-bit microcontroller technology make it possible for devices in any cost or application segment to communicate and be managed end-to-end securely from local and remote services. This trend will continue to bring both the price and power consumption of Internet connected devices down.

Constrained IP based devices and networks are being deployed across the entire range of market segments for M2M, from streetlights and electric meters to home and building automation systems. In addition to technical benefits of re-using IP infrastructure and end-to-end security, there is a very concrete business case for the deployment of device management and application data standards like Lightweight M2M. For example, the ratio of non-Cellular to Cellular (or broadband) devices in a typical outdoor lighting or metering application is greater than 500:1,

often 100:1 in building automation and 20:1 in home automation. Thus it makes sense to extend the current approach to M2M management and application services beyond Cellular or broadband-based devices. Lightweight M2M together with inevitable shift towards IP based networks opens up a much larger market for everyone in the ecosystem.

3. OMA Lightweight M2M Overview

The OMA Lightweight M2M Enabler (LWM2M) is targeted in particular at constrained devices, e.g. devices with low-power microcontrollers and small amounts of Flash and RAM over networks requiring efficient bandwidth usage. At the same time, LWM2M can also be utilized with more powerful embedded devices that benefit from efficient communication. LWM2M provides a light and compact secure communication interface along with an efficient data model, which together enables device management and service enablement for M2M devices. As with other device management standards such as OMA DM, the Lightweight M2M solution is called an Enabler.

The LWM2M Enabler defines the application layer communication protocol between a server and a client. The LWM2M Server is typically located in a private or public data centre and can be hosted by the M2M Service Provider, Network Service Provider or Application Service Provider. The LWM2M Client resides on the device and is typically integrated as a software library or a built-in function of a module or device. Four logical interfaces are defined between server and client namely, 1) Bootstrap, 2) Device Discovery and Registration, 3) Device Management and Service Enablement, and 4) Information Reporting. The LWM2M architecture is shown in Figure 2.

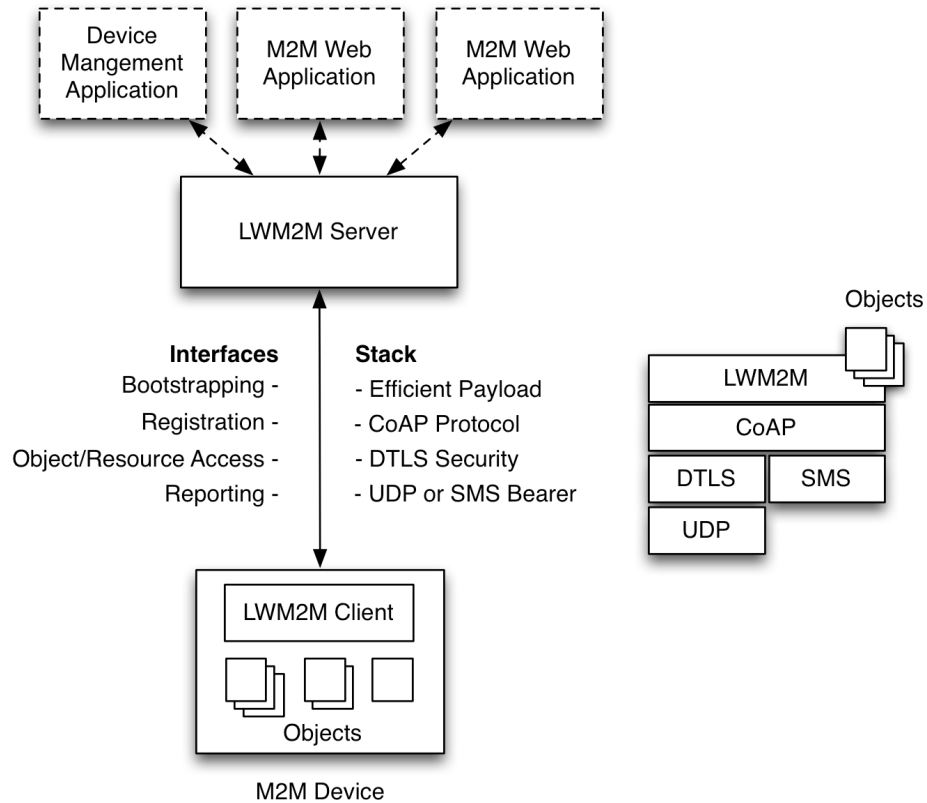


Figure 2 The Lightweight M2M architecture with LWM2M Server and LWM2M Client

The LWM2M protocol stack [2] utilizes the IETF Constrained Application Protocol (CoAP) [3] as the underlying transfer protocol over UDP and SMS bearers. CoAP defines the message header, request/response codes, message options, and retransmission mechanisms. The CoAP protocol was defined by the IETF Constrained RESTful Environment (CoRE) working group. The main goal for the CoRE working group was to keep message overhead small, limit fragmentation, support multicast and create a simplistic protocol for M2M.

CoAP creates an alternative to HTTP for RESTful APIs on resource-constrained devices and supports the basic methods of GET, POST, PUT, DELETE (as with HTTP), which are easily mapped to those of HTTP. Unlike HTTP, CoAP messages are exchanged asynchronously between CoAP end-points over a datagram-oriented transport such as UDP. A subset of response codes are supported for LWM2M response message mapping. Built-in resource discovery is supported using the CoRE Link Format standard. CoAP messages are encoded in a simple binary format, allowing this functionality starting with just a 4-byte overhead. LWM2M defines the UDP Binding with CoAP as mandatory whereas the SMS Binding with CoAP is optional. This means, that LWM2M client-server interaction can happen both via SMS and UDP.

The LWM2M includes state of the art security to secure communications between client and server using Datagram Transport Layer Security (DTLS) [4]. DTLS is used to provide a secure channel between the LWM2M Server and the LWM2M Client for all the messages interchanged. DTLS security modes include both pre-shared key and public key technology to support both very

limited and more capable embedded devices. The LWM2M standard defines provisioning and bootstrapping functionality that allows a LWM2M Bootstrap Server to manage the keying, access control and configuration of a device to enrol with a LWM2M Server. The security identifiers, endpoint identifiers and keys are used uniformly throughout the LWM2M system to provide a complete security lifecycle solution.

As mentioned earlier, the LWM2M Enabler defines a simple resource model where each piece of information made available by the LWM2M Client is a Resource². The Resources are further logically organized into Objects. The LWM2M Client can have any number of Resources, each of which belongs to an Object. For example the Firmware Object contains all the Resources used for firmware update purposes. Figure 3 illustrates the structure and relationship between Resources, Objects, and the LWM2M Client.

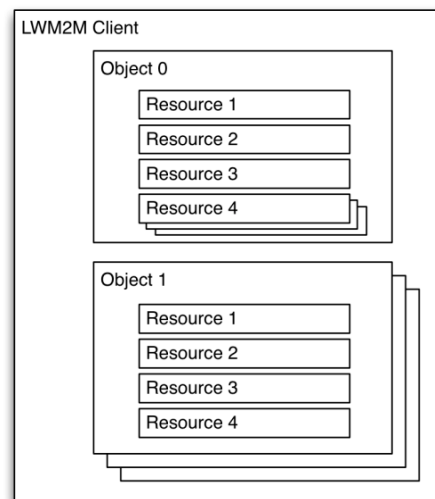


Figure 3 The LWM2M Object model

The first release of the OMA LWM2M standard specifies, in addition to the Enabler itself, an initial set of objects for device management purposes:

- **LWM2M Security:** to handle security aspects between management servers and the LWM2M client on the device.
- **LWM2M Server:** to define data and functions related to the management servers
- **Access Control:** to define for each of several permitted management servers the kinds of access rights they have for each data object on the client.
- **Device:** to detail resources on the M2M device related to device specific information.
- **Firmware:** to detail resources on the M2M device useful for firmware upgrades.
- **Location:** to group those resources that provide information about the current location of an M2M device.

² As in the REST architectural style.

- **Connectivity monitoring:** to group together resources on the M2M device that assist in monitoring the status of a network connection.
- **Connection statistics:** to group together resources on the M2M device that hold statistical information about an existing network connection.

As an example, the device object allows remote retrieval of device information such as manufacturer, model, power information, free memory, and error information. Furthermore, the device object provides a resource for initiation of a remote reboot or factory reset. Another example is the firmware object, which provides all resources needed to enable firmware updates.

A typical message flow between a LWM2M Client and Server is depicted in Figure 4.

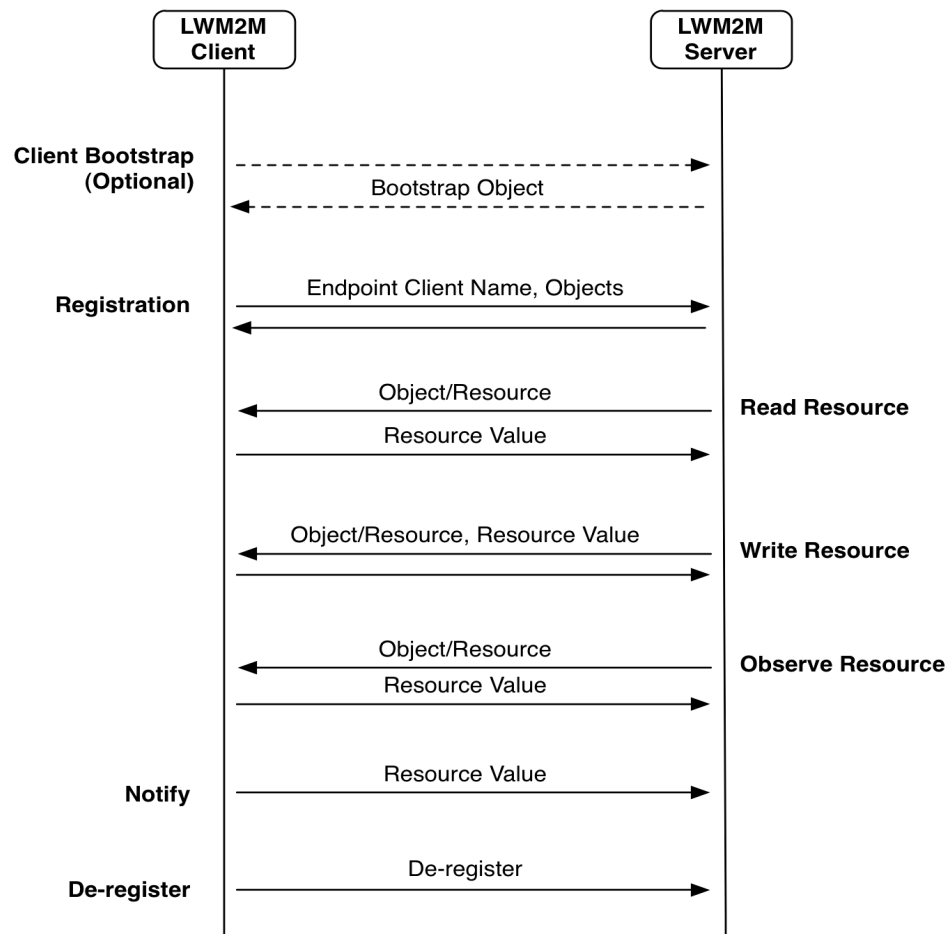


Figure 4 Abstract message flow example between a LWM2M Client and Server, the actual messages are mapped to CoAP requests and responses

The abstraction between the underlying transfer protocol with the simple CoAP GET, PUT, POST, DELETE commands and the LWM2M data model is one of the greatest benefits of LWM2M. It allows nearly unlimited extensions to the data model enabling any kind of functionality for any kind of M2M use cases. For example the IPSO Alliance has already created compatible object descriptions related to smart city applications. Furthermore, any organization or

company can create new compatible objects that widen the scope of addressable M2M devices and appliances. The OMA will soon launch a public web site where these Objects are available and can be registered free of charge.

Future versions of the LWM2M protocol will address further evolving requirements of the Internet of Things. New features could include e.g. a CoAP/TCP binding for LWM2M and further LWM2M objects to enable even more device management use cases.

4. Benefits

The LWM2M standard solves a set of technological challenges that have appeared as the M2M market has matured and the Internet of Things makes constrained devices more accessible to device management and end-to-end service enablement. In this section we summarise the benefits of LWM2M:

- Greater market growth and cost efficiency for the whole industry through a decoupling of devices, device management and services technologies.
- Service providers, OEMs and end users benefit from the uniform management of constrained devices.
- Compared to the protocol stacks used with traditional mobile devices, LWM2M can often provide a 10x increase in efficiency.
- Better time to market for M2M services, as well as devices and infrastructures through standard components available from an ecosystem of vendors.
- LWM2M is complementary to existing device management solutions like OMA DM and Broadband Forum TR-69, and greatly extends the range of devices that can be securely managed.
- The LWM2M data model and the open OMA naming authority registry for Objects provide easily accessible and reusable semantics for both device management and application data for the whole Internet of Things industry.
- By providing a single solution for both device management and application data, LWM2M both simplifies systems and allows for new and innovative M2M services.
- Complete security and security lifecycle management appropriate for constrained devices solves one of the most pressing problems in the M2M industry.
- The scope of LWM2M defines only the device to service network interface, allowing easy integration into existing device management and M2M services, as well as larger backend system standards such as oneM2M.

5. Comparison with Other Approaches

The LWM2M solution complements existing standards for device management. A comparison of the traditional OMA DM used for mobile and gateway management and Lightweight M2M is provided in Table 1. Whereas OMA DM is clearly suitable for more powerful devices with broadband Cellular

communication, OMA LWM2M supports a low-overhead communication model with simple objects. LWM2M is applicable to the transfer of application data in addition to device management. In systems with a gateway already under device management using OMA DM, it would be possible to manage local IP-based devices using LWM2M with the OMA DM Gateway Management Object. The TR-69 standard for the management of fixed cable and broadband modems and gateways, is comparable to LWM2M in a similar way.

Other general-purpose protocols are sometimes applied for communication for embedded and mobile devices. These include HTTP, XMPP and MQTT to name a few, which are all TCP based. A protocol as such is just a mechanism for transferring information, and provides limited value on its own. A protocol typically lacks security, security lifecycle management, interoperable system interfaces, data formats, data definitions for device management – all of which are provided by a complete standard like LWM2M. In addition these protocols were designed with connection oriented PCs, mobile and powerful embedded devices and non-constrained networks in mind and are thus aimed at solving a different set of problems in the first place. LWM2M is based on CoAP, which was designed specifically with the security and communication needs of constrained devices and networks in mind. Around that LWM2M provides a complete, interoperable solution for security management, device management and service enablement.

Table 1 Comparison of traditional device management and Lightweight M2M

	OMA DM	OMA LWM2M
Transport	HTTP, WSP, and OBEX bindings	COAP over UDP and SMS bindings
Communication Model	More complex with OMA DM protocol packages (package 0-4)	Registration followed by simple COAP GET, PUT, POST, DELETE
Data Model	DM tree with often very complex Management Objects. Server needs to know management tree structure of each device before it can manage.	Flat, simple objects with uniform URI across devices
Message Overhead	HTTP + XML Messages (100s of bytes)	CoAP + binary encoded TLV or JSON (10s of bytes)
Application Data?	No	Yes
Device Applicability	Mobile phones, tablets and M2M gateways	Constrained local wireless or M2M Cellular based devices

6. Go to Market and Ecosystem Aspects

Whenever a new standard is created, it takes some time until a significant market penetration is reached and it is available on a wide range of products. However, M2M enterprise customers, M2M system integrators, service providers, and application developers are already able to benefit from the advantages of LWM2M today. For example there are already companies providing the software to build LWM2M servers and to embed clients into M2M devices. Furthermore, open source implementations exist supporting developers in creating compelling M2M applications. Some M2M application providers are ready to offer comprehensive server solutions and early-mover device vendors are planning to bring LWM2M-enabled modules and devices to the market soon.

The creation of an ecosystem around LWM2M has started. The IPSO Alliance [5] is defining LWM2M objects for smart city/building applications. This makes the job easier for M2M solution designers. In addition, any company can define their own objects and either suggest them for standardization to OMA, or use them as their company-proprietary objects without standardisation. Furthermore, a LWM2M open source project has been started at the Eclipse Foundation [6].

The Open Mobile Alliance is also supporting the ecosystem creation by measures such as various promotional activities around LWM2M including webinars and speaking engagements at industry events. Furthermore, OMA is developing a test suite that can be used for any testing purpose including device certification. Another activity is the organization of Test Fests in the context of the OMA interoperability program. The first LWM2M test event was held with ETSI and the IPSO Alliance in November 2013 in Las Vegas and attracted both industry and open source players who have implemented CoAP and/or LWM2M [7].

Furthermore, the OMA is creating a web tool aiming at making it easy for developers to create new LWM2M objects to support their desired use cases. The tool will also allow the conversion of objects into machine-readable code and object registration for obtaining a unique object ID.

7. References

- [1] Analysys Mason, M2M Device Connections and Revenue: Worldwide Forecast 2013-2023, August 2013
- [2] "OMA Lightweight Machine to Machine Protocol v1,0"
http://technical.openmobilealliance.org/Technical/release_program/lightweightM2M_v1_0.aspx
- [3] Shelby, Z., Hartke, K., Bormann, C., and B. Frank, "Constrained Application Protocol (CoAP)", draft-ietf-core-coap-18 (final), June 2013.
- [4] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", [RFC 6347](#), January 2012.
- [5] IPSO Alliance <http://www.ipso-alliance.org/>
- [6] Eclipse Foundation <http://www.eclipse.org/>
- [7] Joint ETSI/IPSO Alliance/OMA Test Event on CoAP and LWM2M, Nov 2013, Las Vegas, Test Report, :
http://member.openmobilealliance.org/ftp/Public_documents/IOP/2014/OMA-IOP-2014-0003-INP_CoAP3_LWM2M_Plugtest_Test_Report_V1_0.zip

8. About the Authors

Guenter Klas, Vodafone

Guenter Klas is currently Head of Research & Architecture with Vodafone Group R&D. More recently Guenter has been driving research and system architecture work related to M2M, with a focus on remote management for smart metering and smart grid. His other fields of research range from exposure of network functions through APIs to next generation communications and cloud computing in a mobile context. Guenter has also been leading several of Vodafone's standardisation and co-operation engagements in organisations like OMA, W3C and GSMA.

Before joining the Vodafone Group Technology function, Guenter led a system design group at the Vodafone UK operating company and previously held various product management, product development and research management roles at Siemens. Guenter has produced numerous publications, holds a MSc degree in Electrical Engineering and a PhD in Computer Science.

Friedhelm Rodermund, Vodafone

Friedhelm Rodermund is Senior Standards Strategist at the Vodafone Innovation Park, Germany, where he is currently focusing on the development of standards and products for the internet of things. He is the technical editor of the OMA Lightweight M2M specification and a key contributor. Furthermore, he has been leading the development of LWM2M prototypes which took place jointly with industry partners.

As a widely recognized telecoms expert he was actively involved in leading roles in the development of key standards for mobile telephony and mobile data across standards development organizations such as OMA, ETSI, 3GPP, GSMA and oneM2M. He holds several patents, has published numerous articles and has contributed to various technical books.

Zach Shelby, ARM

Zach Shelby is Director of Technology for Internet of Things at ARM and a thought leader for the whole industry. Zach was co-founder of Sensinode where he has acted as CEO and CTO for the ground-breaking company before recent acquisition by ARM. Before starting Sensinode, he led wireless networking research at the Centre for Wireless Communications and at the Technical Research Center of Finland.

Zach is a key contributor at the IETF for IoT standards with contributions in 6LoWPAN, routing, web services and security related standards, ETSI and OMA standardisation on M2M, and in several top international research programs. Zach is known as a pioneer in the use of IP and Web technology in low-power networks with 6LoWPAN and CoAP standards development, and is co-author of the book "6LoWPAN: The Wireless Embedded Internet". His results include a large portfolio of courses, publications, public talks, broad research cooperation, and key patents. Zach

has served on the Technical Advisory Board and currently on the Board of Directors at the IPSO Alliance.

Sandeep Akhouri, Ericsson

Sandeep is the Chief Architect for the Ericsson Remote Device Management product that provides M2M services through automated settings, service provisioning, monitoring and fault handling for wireline and wireless devices. He leads the Ericsson Device Management standardization activities in OMA. He works across industry verticals including Utility, Smart Cities and transportation.

He has published articles at several leading conferences on M2M, ZigBee and Big Data Analytics.

Jan Höller, Ericsson

Jan Höller is a Principal Researcher at Ericsson Research where he has a responsibility to define and drive technology and research strategies. He established Ericsson's research activities in the Internet of Things almost a decade ago, and has since then continued to contribute to the company strategies in the area of M2M and Internet of Things towards the Ericsson vision of "50 Billion connected devices" in the Networked Society. He has been active in a number of international research programmes on the Internet of Things, and is co-author of the book "From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence". He also serves as secretary on the Board of Directors at the IPSO Alliance.

Jan has held various positions in Strategic Product Management, Technology Management and has since he joined Ericsson Research in 1999 led different research activities and research groups. He has produced publications, public presentations, technical book contributions and holds several patents.