LwM2M in ENISA's Secure Supply Chain for IoT

Approved Version: - 2021-05-11

Open Mobile Alliance

OMA-WP-ENISA-LwM2M-20210511-A

Master: 18 May 2021 23:24:00 *rev: d8f0059*

Table of Contents

Table of Figures

Table of Tables

1. Introduction

Formed in 2002, the Open Mobile Alliance (OMA) combined several industry fora working on mobile application protocols. It is a standard developing organization, which develops interoperable protocols. In late 2017, OMA merged with the IPSO Alliance to form a new organization called OMA SpecWorks. Within OMA SpecWorks the technical work is conducted in several working groups. One of those groups develops the Lightweight Machine-to-Machine (LwM2M) protocol to manage Internet of Things (IoT) devices over their entire lifecycle.

When the European Union Agency for Cybersecurity (ENISA) published their guidelines for a secure IoT supply chain late 2020, were curious as to the role the LwM2M, standardized IoT device management protocol, has in enabling security in the supply chain. This whitepaper is the result of our investigation.

Our findings are that the use of LwM2M provides security benefits through all supply chain stages. It is worthwhile to note that distinctions need to be made between the specification defining the LwM2M protocol, the implementation of the LwM2M protocol in IoT devices and in a device management platform, and the use of the implementation in a specific deployment environment.

2. LwM2M in a Nutshell

OMA SpecWorks' LwM2M specification evolved from its OMA DM standardization used in smart phones. Originally proposed in 2012, LwM2M v1.0 was finally published in early 2017 after comprehensive research with developers across multiple industries and application areas. LwM2M defines a messaging protocol between the LwM2M server infrastructure and LwM2M clients in IoT devices. LwM2M also defines a data model, which is used to offer semantic interoperability of the data exchanged between IoT devices and their management infrastructure. Hence, LwM2M is also used for exchanging application data. The latest version of LwM2M v1.0 is v1.0.2 and it was published in February 2018.

LwM2M v1.0 uses the Constrained Application Protocol (CoAP) over UDP and SMS to provide the transport for the LwM2M messages, with operations to create, update, delete, and retrieve resources. In addition to the messaging, a core set of objects were defined, which can be encoded in different data formats. Provisioning of security credentials and access control lists is offered by a dedicated LwM2M bootstrap server, a form of a key distribution server.

Figure: 2.-1 LwM2M Protocol Architecture shows the overall architecture of the LwM2M protocol.

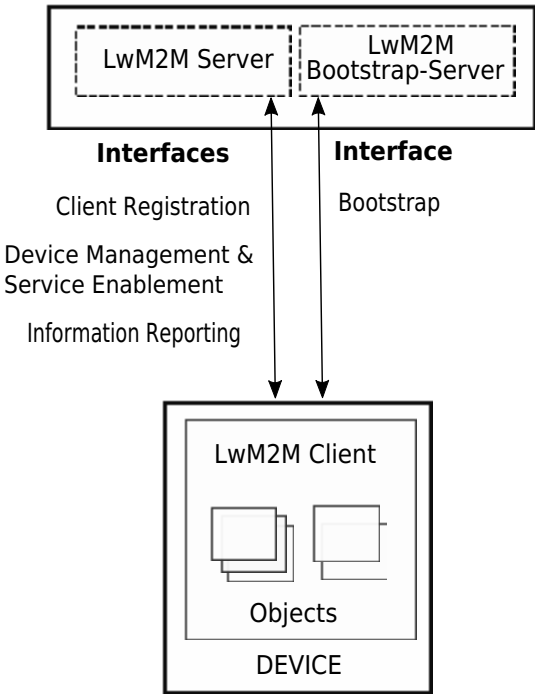

Figure: 2.-1 LwM2M Protocol Architecture

For communication between the LwM2M enities, four RESTful interfaces are defined in LwM2M v1.0: three between the LwM2M Client and the LwM2M Server (Client Registration, Device Management & Service Enablement, and Information Reporting) and one interface for use between the LwM2M Client and the LwM2M Bootstrap Server for credential provisioning (called bootstrapping).

LwM2M provides the following capabilities:

- Key management and provisioning of access control lists,
- Reading sensor data,
- Trigger actuators,
- Device configuration,
- Software and firmware update,
- Report reporting, and
- Fault Diagnostics

LwM2M is a mature technology - not only from a standardization point of view but also from an interoperability testing and deployment angle. Below is a short summary of how the specification evolved over time. Each version advanced with new features requested from users of the technology and with feedback from developers.

LwM2M v1.1 was published in July 2018 and split the specification into two: a core specification defining the LwM2M messaging and a transport specification. This was done to put a stronger emphasis on the independence of the LwM2M messaging from the underlying transports. New transports were added to support LwM2M to manage low power, wide area network devices, such as 3GPP NB-IoT and LTE-M as well as LoRaWAN. CoAP over TLS/TCP was added as well.

Figure: 2.-2 LwM2M v1.0.x Protocol Stack and Figure: 2.-3 LwM2M v1.1.x Protocol Stack show the protocol stacks of LwM2M v1.0.x and LwM2M v1.1.x, respectively.

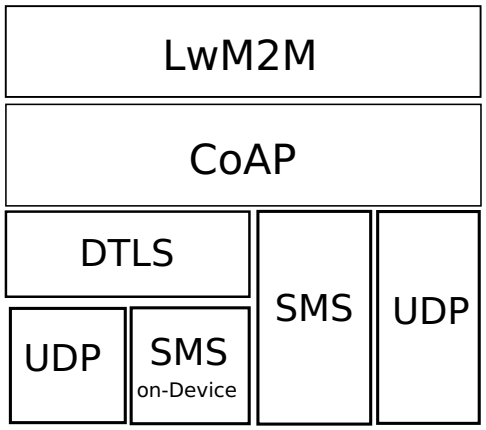

Figure: 2.-2 LwM2M v1.0.x Protocol Stack

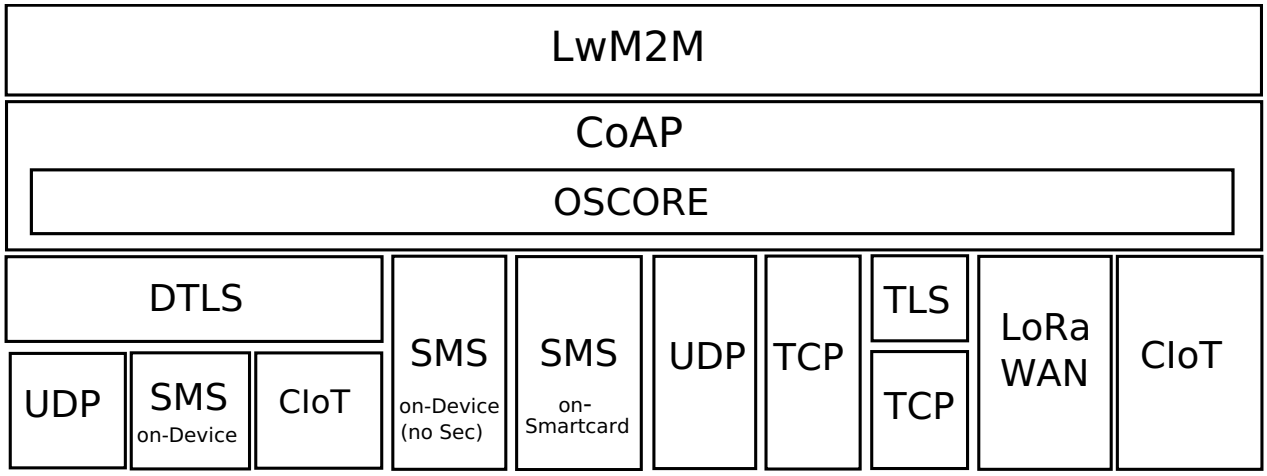

Figure: 2.-3 LwM2M v1.1.x Protocol Stack

The latest version of LwM2M 1.1 is v1.1.1, which was published in June 2019.

Over the years, the OMA SpecWorks has worked with the developer community and received suggestions for optimizations. Published in November 2020, version 1.2 is backwards compatible to LwM2M version v1.0 and v1.1 with respect to mandatory features. Based on feedback received from the LwM2M development community, LwM2M v1.2 includes various new features, such as new transports (MQTT and HTTP), support for LwM2M gateways, and performance optimizations.

Figure: 2.-4 LwM2M v1.2.x Protocol Stack show the protocol stack of LwM2M v1.2. Note the number of transports supported by the LwM2M protocol, which makes it suitable for a range of deployment environments.

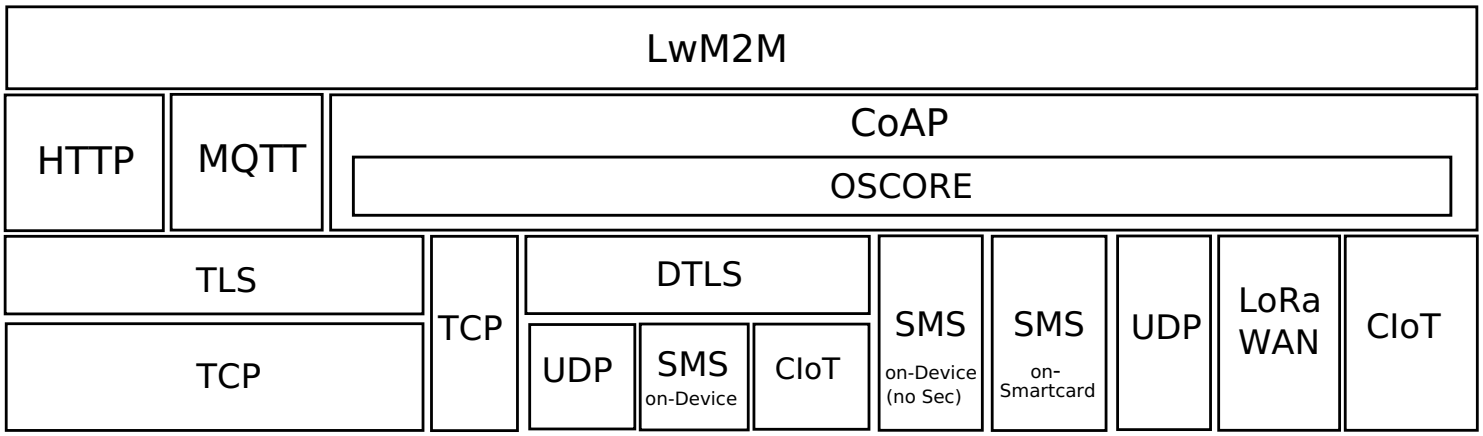

Figure: 2.-4 LwM2M v1.2.x Protocol Stack

3. LwM2M and its part in the (ENISA) Secure Supply Chain

The European Union Agency for Cybersecurity (ENISA) published their Guidelines for Securing the Internet of Things (IoT) – Secure Supply Chain for IoT, in November 2020. We used this document to analyze how its LwM2M met these guidelines - not only to improve the security of the IoT supply chain in general, but to improve security in the development of LwM2M.

The ENISA document addresses the entire supply chain across the IoT ecosystem. The LwM2M protocol is a part of that ecosystem. In the analysis, we address the stages of the supply chain reference model as well as applied those stages to the development cycle of a standardized protocol. Some areas of the reference model were a better fit than others, but the intent was to leverage ENISA's work to the fullest extent possible – not only to give the LwM2M development community and users a view of LwM2M security, but also to identify areas for potential improvement in LwM2M's security and usefulness.

The stages in the secure supply chain are shown in Figure: 3.-1 IoT Supply Chain Stages, a diagram taken from the ENISA recommendation.

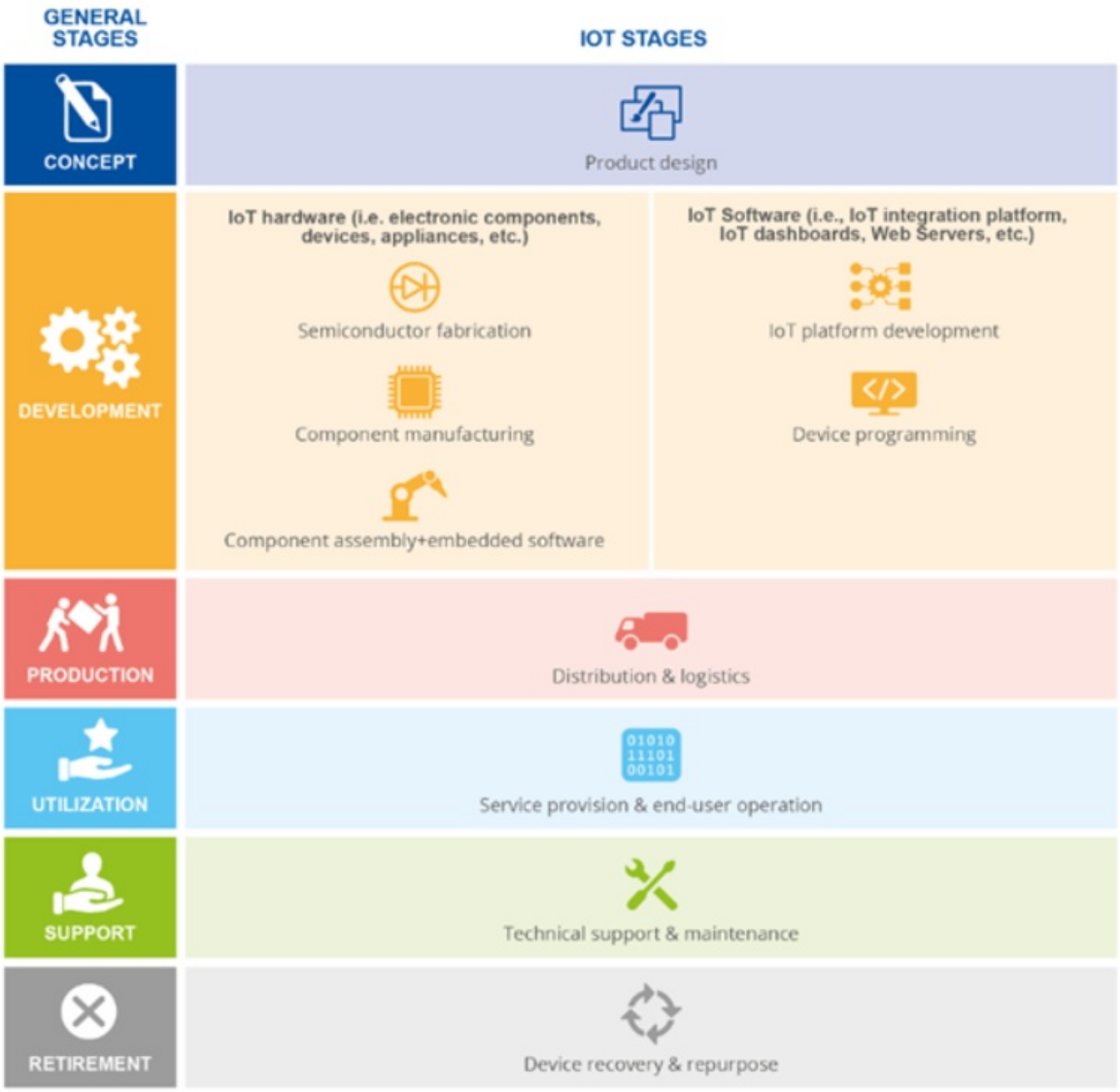

Figure: 3.-1 IoT Supply Chain Stages

3.1. Stage 1 – Concept/Product Design

While the LwM2M protocol can be considered a "product", in ENISA's stages shown in Figure: 3.-1 IoT Supply Chain Stages, it is the rule set describing the format and exchange of data between the LwM2M client and servers. Developers then use the protocol to create software for their products, which is part of the IoT supply chain ecosystem described by ENISA.

From the beginning of LwM2M v1.0 development, we used the classical Internet threat model [RFC3552] as the basis with some modification for smart card usage. We also inherit security models used by our referenced specifications and protocols. The IoT threat landscape has evolved since 2012, so now that v1.2 is published, a review of our security threat model may identify new or changed threats.

Protection of personal data, also called Personally Identifiable Information (PII) in some regions, deserves appropriate protection, which can be accomplished using the communication security and access control mechanisms offered by

LwM2M. One important consideration for privacy is the storage of IoT device data in the LwM2M servers since unauthorized access and leakage of such data must be avoided. The use of PII assumes a linkage to humans using IoT devices. The LwM2M protocol itself does not link users to IoT devices, this may happen in deployments using adjacent technologies. It is therefore the responsibility of companies managing IoT devices to take adequate security measures to respect privacy of their users.

Security threats depend on the implementation and the deployment of the software. We respond when the LwM2M development community raises security issues that need to be addressed by the protocol.

3.2. Stage 2 – Development

This stage in ENISA's model include all the steps necessary to produce a physical device ready to ship to customers. This includes software development. We liken this to the process to produce a LwM2M protocol version – drafting text, reviews, revisions. OMA SpecWorks organizes TestFests to ensure that interoperability between different vendor implementations is accomplished and we receive feedback from these TestFests.

In each LwM2M version, we include support for the state-of-the-art security algorithms and protocols. There is, however, the need to support older algorithms (such as AES-CBC) for backwards compatibility reasons. We follow best current practices, such as not supporting passwords and recommending high-entropy secrets.

As a standards developing organization, we do not mandate a specific implementation practice. We specify the protocol. Developers implementing the LwM2M protocol may include imported libraries as part of their product. Since the LwM2M specification uses many specifications developed by other organizations, such as the 3GPP, IETF, Global Platform, there is a bigger chance that software for individual building blocks exists and can therefore be re-used.

The LwM2M specification defines detailed error handling procedures. We have continually enhanced the LwM2M security procedures. Channel security via DTLS was provided since LwM2M v1.0. Support for OSCORE was added in LwM2M v1.1 to provide the capability for CoAP-level security protection. TLS 1.3 and DTLS 1.3 support was added in LwM2M v1.2.

3.3. Stage 3 – Production

This stage in ENISA's model focuses on production, distribution, and logistics – all the activities needed to deliver product and tracking units in IoT devices.

Published versions of LwM2M are publicly available for download at OMA SpecWorks' website and through our Github site.

3.4. Stage 4 – Utilization

This is the use of a product implementing the LwM2M specification for management of IoT devices during their entire lifecycle. Any issues found with the LwM2M protocol can be fed back to our standardization community to add new features or to clarify the specification text.

LwM2M provides capabilities to support device management for IoT devices:

- It supports secure bootstrapping to provide client credentials used to securely communicate with the LwM2M servers
- It supports secure device registration with the LwM2M servers
- It supports secure communications with the LwM2M servers

The one area we identified that seems pertinent to this stage is that our specifications do not describe the transfer of ownership and the implications for the software and credentials on the device. We may address this in a future version.

3.5. Stage 5 – Support

This stage in ENISA's supply chain model focuses on repairing/replacing damaged units and maintaining a device's security (e.g., maintaining updates, remote support). As LwM2M provides device management capabilities, it is designed to support this stage by providing the abilities to configure the device, update the firmware, and complete remote diagnostics.

For the protocol development lifecycle, we accept requests for new features, performance improvements, and bug fixes from our LwM2M development community. We produce bug fix versions (two for v1.0, one for v1.1), although we do not have a self-imposed timeline for these corrected versions.

IoT devices should be upgraded to support newer versions of the LwM2M protocol using the built-in software update mechanism provided by LwM2M. This could include new features and/or updating the level of security.

Notifications of updated specifications happens via our existing communication channels. Involved member organizations, who participate in the specification development, have awareness of upcoming releases and feature roadmaps. When a new version is published, we advertise it to external organizations and developers via OMA SpecWorks' website as well as via our Github site.

In addition to feedback from the LwM2M development community, we use our liaison interaction with other organizations or members participating in other fora to assist in identifying outdated references, protocols, and libraries in specifications in which LwM2M is dependent as well to identify other security issues.

3.6. Stage 6 – Retirement

To retire an IoT device, LwM2M offers the capabilities to remove credentials and to reset the device to its factory-state.

From a standardization perspective we could either obsolete specifications or stop development of earlier protocol versions. While there are several LwM2M specification versions available already, the protocol is not old enough to retire initial version(s). We do recommend the use of the latest version to developers.

The LwM2M protocol versions have been designed to be backwards compatible so that the server-side infrastructure is able to support different generations of IoT devices.

4. Conclusion

Our analysis concluded that our open standardization process helps with improving security in the following ways:

- Development of the LwM2M protocol is a right granted to OMA SpecWorks members but we offer a way to interact with the wider development community via Github.
- For the work on specification we are also using Github, which enables auditing, and traceability of modifications to our specifications in development.
- Upon completion of the specification, OMA staff reviews the specification and presents it to the Board of Directors for ratification and publication.
- Specifications are publicly available at no cost following the board ratification.
- We use TestFests for testing interoperability of implementations.
- Maintenance involves feedback from developers, results from TestFests, as well as working group discussions.
- Open source implementations of the specification exist, which provide valuable input for developers and researchers.

5. References

[LwM2Mv1.0.2]	OMA, "Lightweight Machine to Machine (LwM2M) Technical Specifications, Version 1.0.2", February 2018. URL: http://www.openmobilealliance.org/release/LightweightM2M/V1_0_2-20180209-A/
[LwM2Mv1.1.1]	OMA, "Lightweight Machine to Machine (LwM2M) Technical Specifications, Version 1.1.1", June 2019. URL: http://www.openmobilealliance.org/release/LightweightM2M/V1_1_1-20190617-A/
[LwM2Mv1.2]	OMA, "Lightweight Machine to Machine (LwM2M) Technical Specifications, Version 1.2", November 2020. URL: http://www.openmobilealliance.org/release/LightweightM2M/V1_2-20201110-A/
[RFC3552]	Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", RFC 3552, July 2003. URL: https://tools.ietf.org/html/rfc3552
[ENISA]	ENISA, "Guidelines for Securing the Internet of Things", November, 2020. URL: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

Table: 5.-1 References