LwM2M v1.1

Lightweight Machine to Machine

Open Mobile Alliance
LightweightM2M (LwM2M) is a Device Management Protocol

H/W Sensors
- Relay (3342)
- Temp (3303)

Driver Sensors
- Switch Drvr
- Temp Drvr

Sensor(s)
- Object/Resource Data Model
- Sensor(s) (3303)
- R-ID
- R-ID
- R-ID
- 5701

Constrained Device
- Client LwM2M
  - 10KB RAM, 100KB Flash, 40 MHZ

Remote Server LwM2M

*Bootstrapping | Device Configuration | Firmware Update | Fault Management | Configuration & Control | Reporting

*Device Management Functions
Data Model
M2M in the Telecom Network: The target for LwM2M Devices

Source: Open Mobile Alliance
LwM2M is recommended for Device Management and Service Enablement because its benefits include:

- Increased bandwidth efficiency based on COAP bandwidth optimization
- Transport-agnostic design that supports UDP, TCP, SMS
- Developer toolkit for application development
- DTLS-based security based on CoAP (IETF)
- Low power client footprint designed for battery constrained devices
- End to end security using IETF OSCORE
Strengths of LwM2M

LwM2M can be used for both data plane (data reporting and devices actuations) and device management.

- LwM2M is a standard defined by OMA
- Suitable for both fixed and mobile devices
- Appropriate for both data plane and device management
- Designed for constrained devices (e.g. < 20 kB RAM)
- Suitable for low powered battery devices because of its low client footprint
- Minimizes bandwidth due to optimized bandwidth consumption by utilizing COAP (COAP is a simplified HTTP; COAP header = 4bytes)
- Simple, stateless protocol
- Crosses FW and NAT systems thanks to support of COAP/UDP and COAP/TCP
- Offers security by design; COAP over UDP or TCP relies on DTLS or TLS respectively
- Provides opportunities for e2e security
LwM2M: Core functionalities

- Bootstrapping
- Device Config.
- Firmware Update
- Diagnostics
- Connection Mgmt.
- Control
- Data Reporting
- Lock & Wipe
Device Configuration
Diagnostics

- Power sources and LwM2M Device settings
- Battery level of the LwM2M Device
- Memory status of the LwM2M Device
- Supported binding modes of the LwM2M Device
- Version of hardware/software of the LwM2M Device
- Capabilities of the LwM2M Device
Connection Management

• Mapping of necessary Cellular and Wi-Fi technologies
• Managing basic parameters needed for the technologies to function e.g. APN, WEP keys etc.
• Adding relevant parameters for bearer selection for cellular connectivity
• Security is covered by DTLS
Control

- Ability to setup access control on Objects for various LwM2M servers
- Wake up the LwM2M Device using SMS
- Reboot the LwM2M Device
- Disable the LwM2M Device for a specified time
- Ask the LwM2M Device to perform registration
Lock & Wipe

![Diagram showing the process of Lock & Wipe involving LwM2M Client and LwM2M Bootstrap Server.]

- **Delete/**
- **PUT /0/1** (Security Object Instance)
- **PUT /1/0** (Server Object Instance)
- **PUT /2/0** (ACL Object Instance)
- **Post / bs**

Server Initiated Bootstrap
LwM2M Security

Types of credential procedures supported
• Certificates
• Pre-shared key
• Public Raw Key
• PKI deployments

Security paths
• DTLS
• SMS
• DTLS over SMS
• OSCORE

LwM2M Security abilities
• Initial keys can be replaced during bootstrap procedure
• Multiple servers could be added with different credentials
• Provide security in every path
LwM2M security – continued

Security Keys

Bootstrap Server

LwM2M Server1

LwM2M Server2

First Contact

Factory Provisioned

Pre-provisioned

Provisioning after First contact

Using Provisioned Credential 1

Using Provisioned Credential 2
LwM2M v1.0 features

- Simple resource model with the core set of objects and resources defined in the specification. The full list of registered objects can be found in the LwM2M registry.
- Operations for creation, update, deletion, and retrieval of resources.
- Asynchronous notifications of resource changes.
- Support for several serialization formats, namely TLV, JSON, Plain Text and binary data formats and the core set of LightweightM2M Objects.
- UDP and SMS transport support.
- Communication security based on the DTLS protocol supporting different types of credentials.
LwM2M v1.0 features continued

• Queue Mode offers functionality for a LwM2M Client to inform the LwM2M Server that it may be disconnected for an extended period of time and also when it becomes reachable again.

• Support for use of multiple LwM2M Servers.

• Provisioning of security credentials and access control lists by a dedicated LwM2M bootstrap-server.
LwM2M v1.1 features

• Improved support for Public Key Infrastructure (PKI) deployments.

• Introduction of enhanced registration sequence mechanisms by the LwM2M Client to LwM2M Server(s).

• Support for LwM2M over TCP/TLS to better support firewall and NAT traversal.

• Support for application layer security for LwM2M based on OSCORE.

• Better support of LwM2M over Low Power WANs, including 3GPP CIoT & LoRaWAN.

• Extended LwM2M commands to enable Resource Instance level access.

• Performance improvement for retrieving and updating Resources of multiple objects.

• Support for JSON using SenML with CBOR serialization for compressed payload with highly efficient transmission.
Enhanced Registration Sequence

Provisioning Server

Client

Bootstrap Server

LwM2M Server 1

LwM2M Server 2

Client powers up; attempt to /bs sending

in endpoint name. /bs srv learns of
endpoint name (IMEI-MSIDN)

/bs srv sends to client srv 1 URL and
credentials, and srv 2 URL and credentials

/bs srv sends back endpoint name, IMSI,
MSIDN, and credentials

Client registers with Srv 1

{mgmt}

Srv1(mgmt) sends network configuration,
APNs, checks firmware etc.

Client registers with Srv 2

{application/repository}

Srv2(application/repository) sends observation
template to client configuring it for operation.
Security & additions to v1.1
Support of LPWAN – 3GPP CIoT

\[\text{LwM2M} \quad \text{CoAP} \quad \text{OSCORE}\]

- **UE**
- **C-SGN**
- **AS**
- **S1-MME**
- **S1-MME (NAS)**
- **SCEF**
- **Non-IP Data**
- **PnP IP Tunnel for non-IP Data**
- **IP Data**
- **SMS**
- **SMSC/IWMSC**

**Network Layers**
- **UDP**
- **SNS on-Device**
- **CIoT**
- **SNS on-Device (no Sec)**
- **SNS on-Smartcard**
- **UDP**
- **TCP**
- **TLS**
- **TCP**

The information in this presentation is public. Copyright © 2019 Open Mobile Alliance
Support of LPWAN – LoRaWAN
Objects from OMASpecWorks

- LwM2M Security
- LwM2M Server
- LwM2M Access Control
- Device
- Connectivity Monitoring
- Firmware Update
- Location
- Connectivity Statistics

- Cellular Connectivity
  - APN Connection Profile
  - WLAN Connectivity
  - Bearer Selection
    - Communication Characteristics
    - Non-Access Stratum (NAS) Configuration
    - LwM2M OSCORE

- Lock and Wipe
- DevCapMgmt
- Portfolio
- LwM2M Software Management
- LwM2M Software Component
- BinaryAppDataContainer
- Event Log
Objects registered OMASpecWorks

- Power Control
- Light Control
- Accelerometer
- Magnetometer
- Barometer
- Altitude
- Load
- Pressure
- Loudness
- Gyrometer

- Addressable Text Display
- Multiple Axis Joystick
- Multi-state selector
- Dimmer

- powerupLog
- radioLinkFailureEvent
- cellBlacklistEvent
- NeighborCellMeasurements
- ServingCellMeasurement
- PagingDRX
- txPowerBackOffEvent
- SipRegistrationEvent
- sipSubscriptionEvent
- VolteCallEvent
- volteCallStateChangeEvent

Refer LwM2M registry for full list -
http://www.openmobilealliance.org/wp/OMNA/LwM2M/LwM2MRegistry.html
# Comparing Equivalent Standards in mobile space

<table>
<thead>
<tr>
<th>Areas</th>
<th>OMA-DM 1.x</th>
<th>LwM2M v1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Management</td>
<td>Established and stable</td>
<td>Growing</td>
</tr>
<tr>
<td>Firmware Updates</td>
<td>Partial Standardized</td>
<td>Partial Standardized and expanding</td>
</tr>
<tr>
<td>Scalability</td>
<td>Targeting bigger devices</td>
<td>Wide Range feasible</td>
</tr>
<tr>
<td>Use in Constrained Devices</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>IoT enablement</td>
<td>Bigger devices feasible but data model needs evolution</td>
<td>Data Model evolved for IoT enablement and is expanding</td>
</tr>
<tr>
<td>Active Standardization members</td>
<td>None</td>
<td>Stable with additional standards working on top</td>
</tr>
<tr>
<td>Service Enablement</td>
<td>Limited to Telecom Features</td>
<td>Expanding into other IoT/verticals</td>
</tr>
<tr>
<td>Service level standardization</td>
<td>- NA -</td>
<td>IRTF T2TRG actively collaborating to expand semantic interoperability on top of LwM2M (OCF, W3C WoT, Fairhair Alliance)</td>
</tr>
<tr>
<td>Supporting Standardization Groups</td>
<td>GSMA, 3GPP</td>
<td>GSMA, IPSO (assimilated into OMA), IETF, IRTF, OpenAIS, oneM2M and expanding..</td>
</tr>
</tbody>
</table>
Status with Industry & market

➢ ARM
➢ AVSystem
➢ Cumulocity
➢ Ericsson
➢ Friendly Technologies
➢ Gemalto
➢ Huawei
➢ IOTECC
➢ IoTerop

➢ Itron
➢ Nokia
➢ Orange
➢ Qualcomm
➢ Sierra Wireless
➢ Smith Micro
➢ Telit
➢ u-blox

Note: A large number of companies around the world are working on LwM2M implementations including many small and medium sized companies.
LwM2M Forecast

• 235 million of LwM2M-enabled devices are expected to be deployed by 2022
  • “IDATE explored the market opportunities over four markets including automotive, utilities, building automation and logistics. The total installed base of LwM2M-enabled devices will reach over 235 million units in 2022, from less than 0.5 million units in 2015,” said Samuel Ropert, Head of IoT Practice at IDATE Digiworld. “This represents a CAGR of 154% in the 2015-2022 period.”

https://www.omaspecworks.org/oma-lightweightm2m-v1-0-approved-by-board-of-directors/