



oma

Open Mobile Alliance
For a Connected World

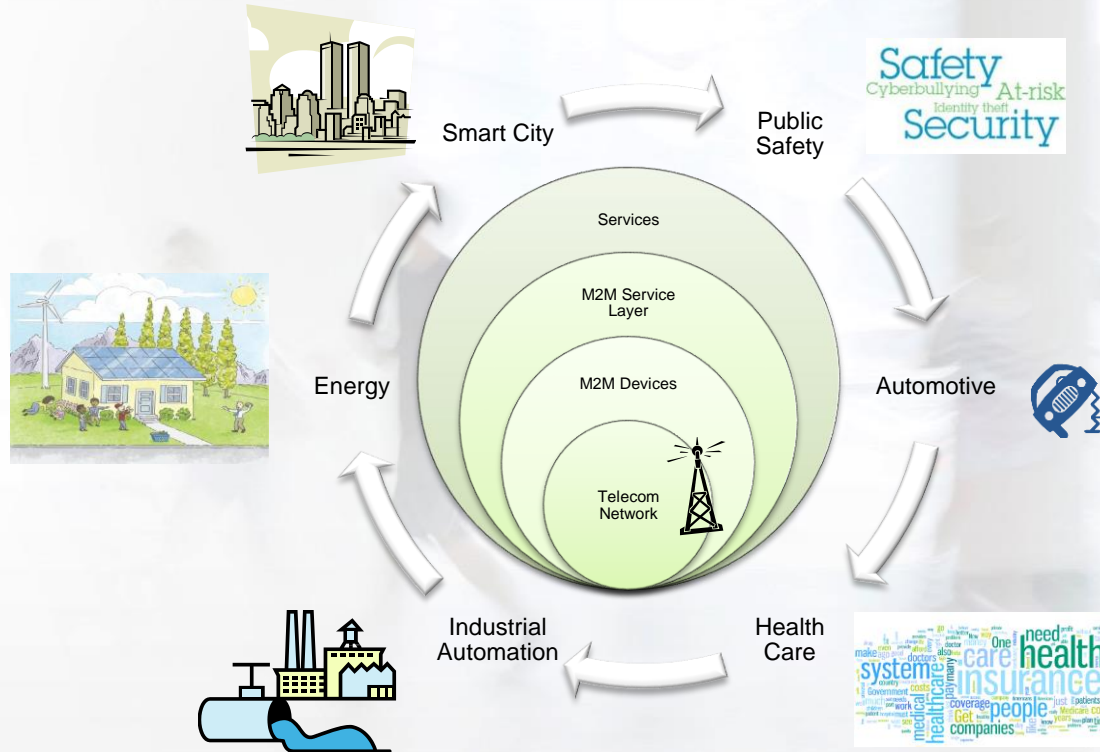
WORKSHOP ON IOT SEMANTIC/HYPERMEDIA INTEROPERABILITY

a LwM2M perspective

Padmakumar Subramani, OMA DM Working Group Chairman

[OMA HELP](#)

M2M IN THE TELECOM NETWORK: THE TARGET FOR LwM2M DEVICES



➤ Org's and usage of LwM2M

- IPSO Objects on LwM2M
- oneM2M integrating LwM2M in its architecture blocks
- GSMA integrating LwM2M as device management protocol for MIoT project

- XML based approach for object and resource definition
- Certain data types are supported in v1_0
- Execution type is possible

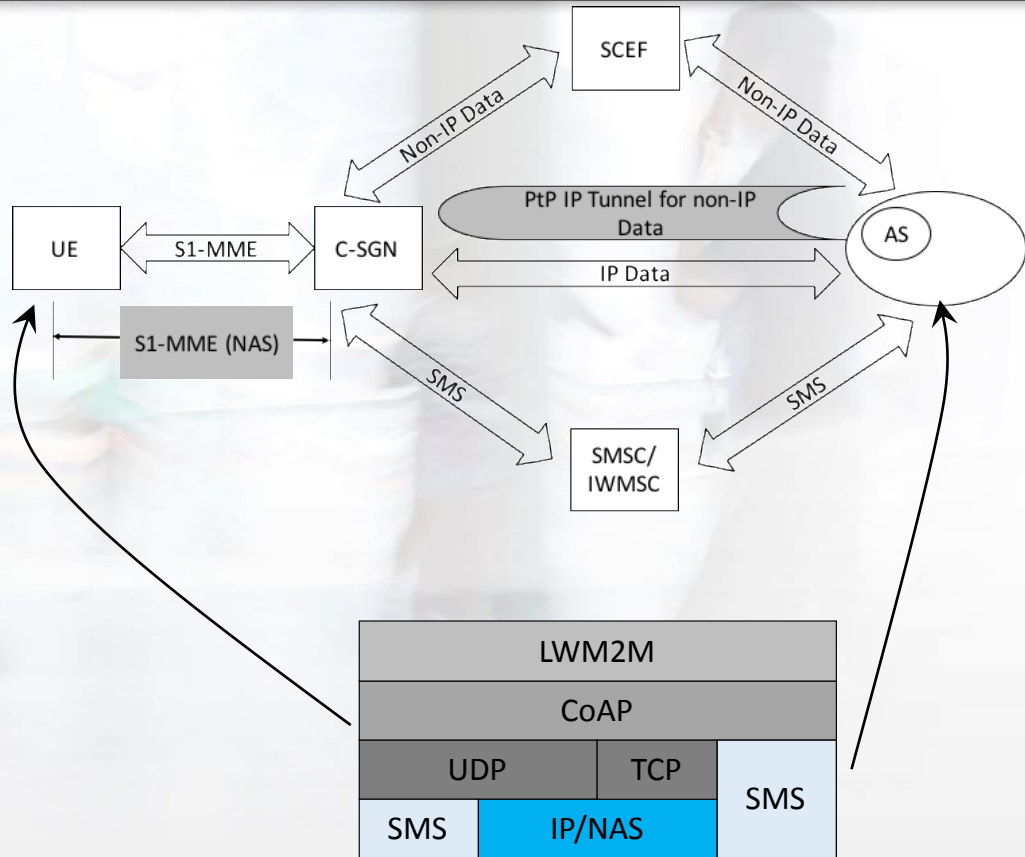


- OMNA registry for aggregation of objects, resources with allocated bands on type of registrations
 - Object Versioning is supported
- Plugfest is planned at the least twice a year for LwM2M
- LwM2M 1_0 is approved in Feb 2017
 - Maintenance release 1_0_1 is completed, planned to be released in July 2017
- LwM2M 1_1 requirement collection is ongoing
 - Planning to have a candidate approval by Feb 2018

- LPWAN support for 3GPP CIoT adaptations (see next slide), LoRA
- CoAP over TCP/TLS
- Support upgrade safeguards for necessary configurations
- Support ability to gain in one command multiple resources from multiple objects and instances
- Improvements to bootstrap and registration interfaces
- Legacy Gateway support in LwM2M with device running on BLE etc., behind the LwM2M gateway
- Introduction of secure element in LwM2M server/client ecosystem
- E2E device to LwM2M Server/Application secure packet transfer
- Incorporate group concept between LWM2M Servers and Clients
- Ability to use HTTP2 for non-constrained devices

LwM2M V1.1 FEATURE: 3GPP CIOT (LPWAN) ADAPTATIONS

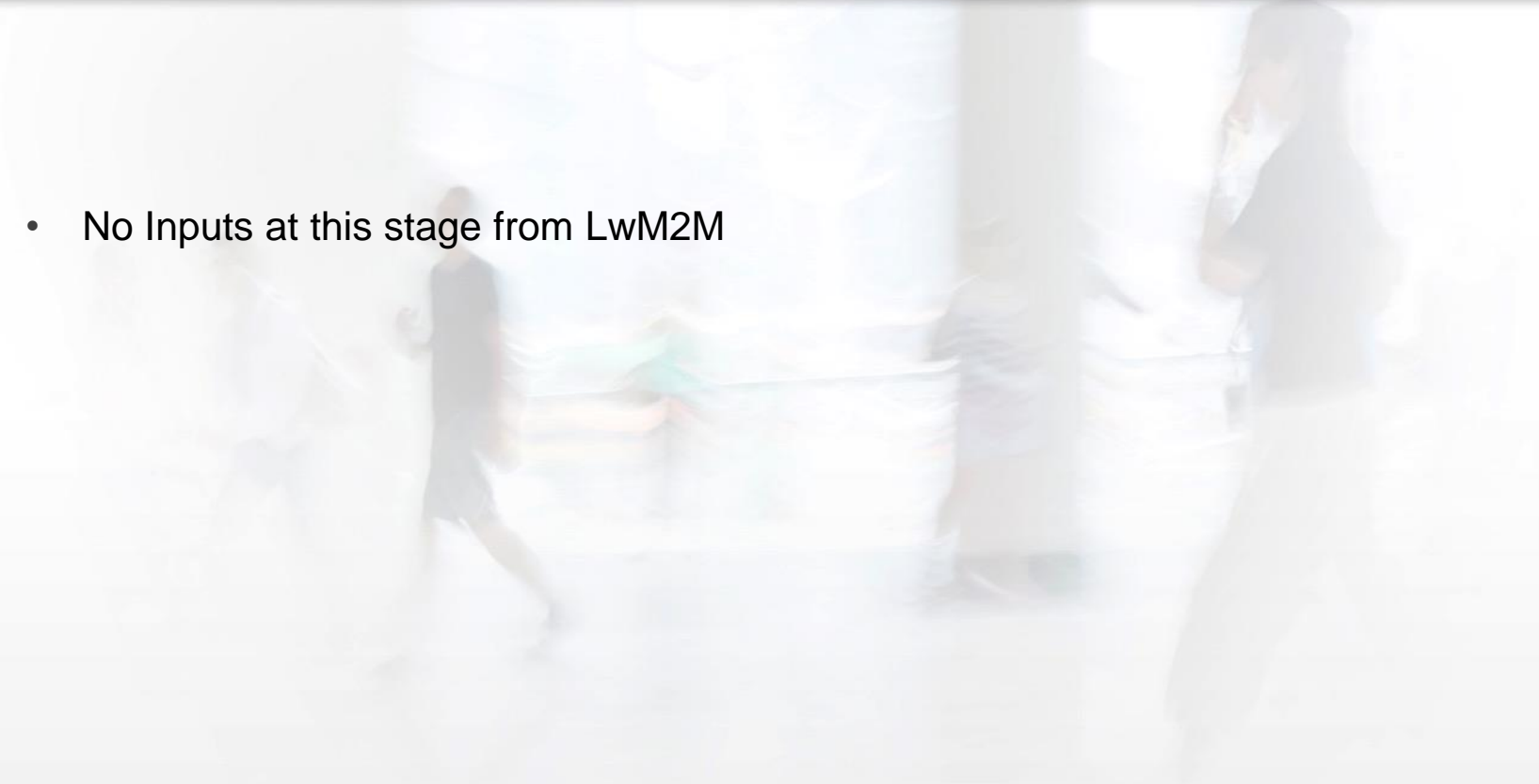
- Provides enablers and device management for delivery of data over the control plane for both Non-IP Data (NIDD) and IP data
- External identifiers support for LPWAN
- Support message identity for data delivery in the control and user planes as well as other applications like Gateways
- Integration of SGI and SCEF paths for NIDD.
- Support delayed/no-acknowledgement methods
- Support rate and byte quotas for devices





- **Organizational view**
 - 2 is happening everywhere in all the standards bodies, which is not ideal situation
 - 3 is ideal, but the discussion to start with 1 and move towards 3 would help the IoT world
- **Semantic missing links**
 - Architectural commonality agreement
 - Dictionaries to come together among various IoT organizations
 - Blocks among various IoT organizations
 - Units are standardized, complexity in service layer is emerging beyond units
 - Service use cases (some good examples are available in ACE)
 - new areas (Analytics/.. ?)
 - Security yardstick - IoT devices

- No Inputs at this stage from LwM2M





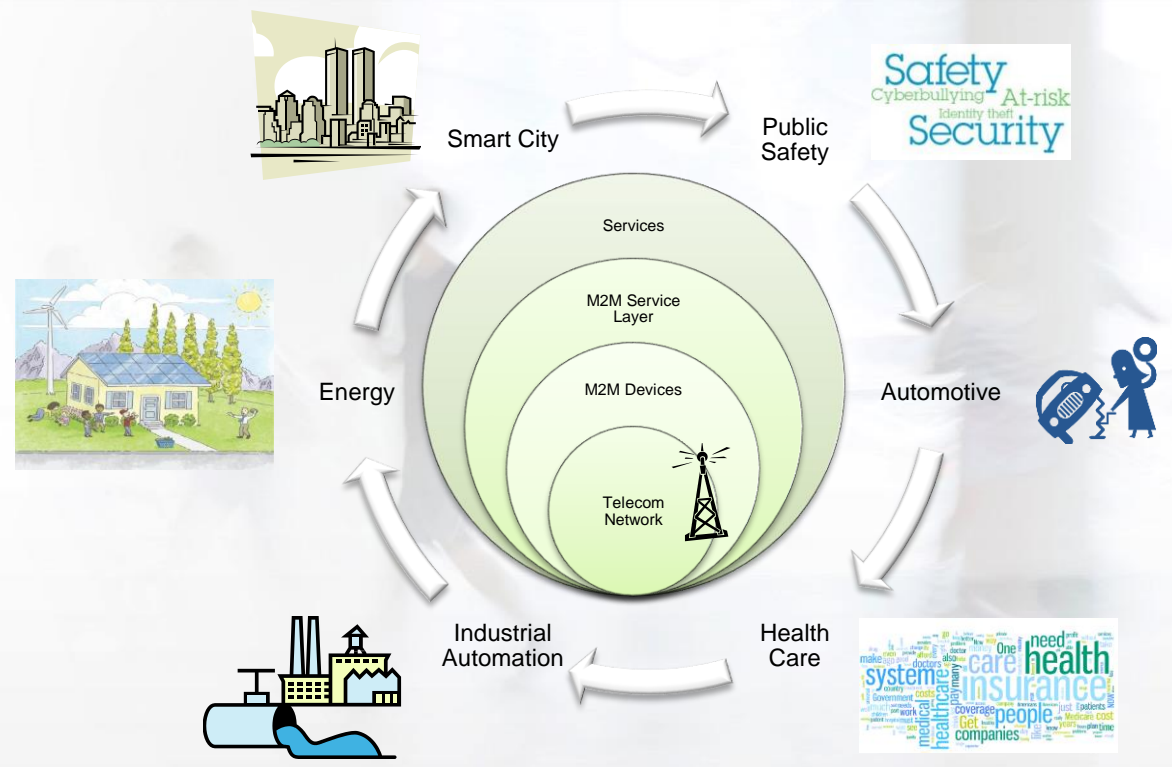
Thank You

[OMA HELP](#)

BACKUP SLIDES

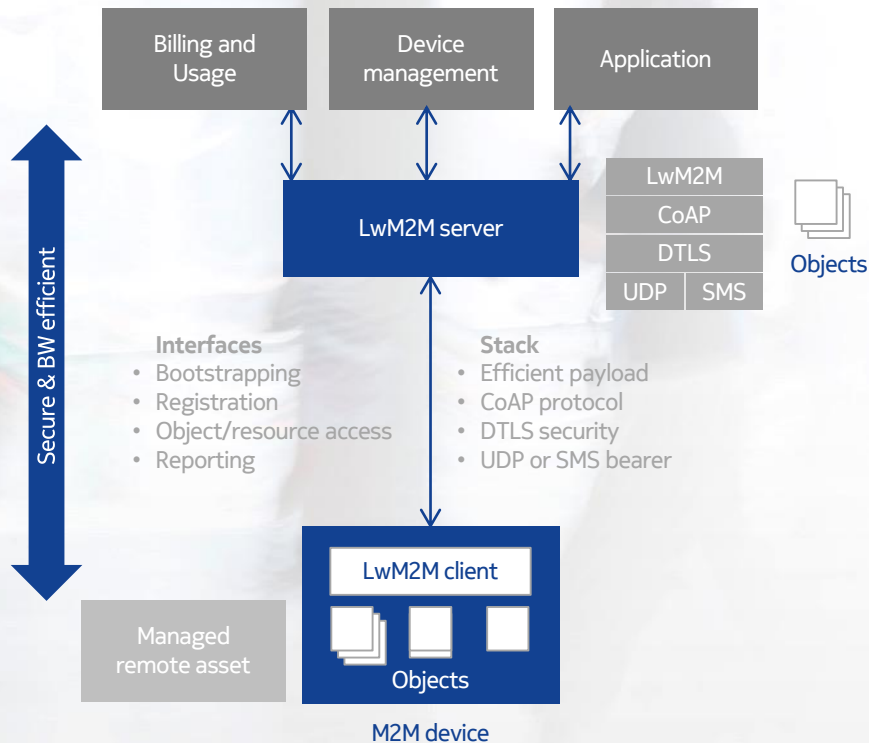


M2M IN THE TELECOM NETWORK: THE TARGET FOR LWM2M DEVICES



OMA recommends utilization of LwM2M for both data plane (data reporting and device actuation) as well as device management due to benefits such as:

- 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 foot print designed for battery constrained devices

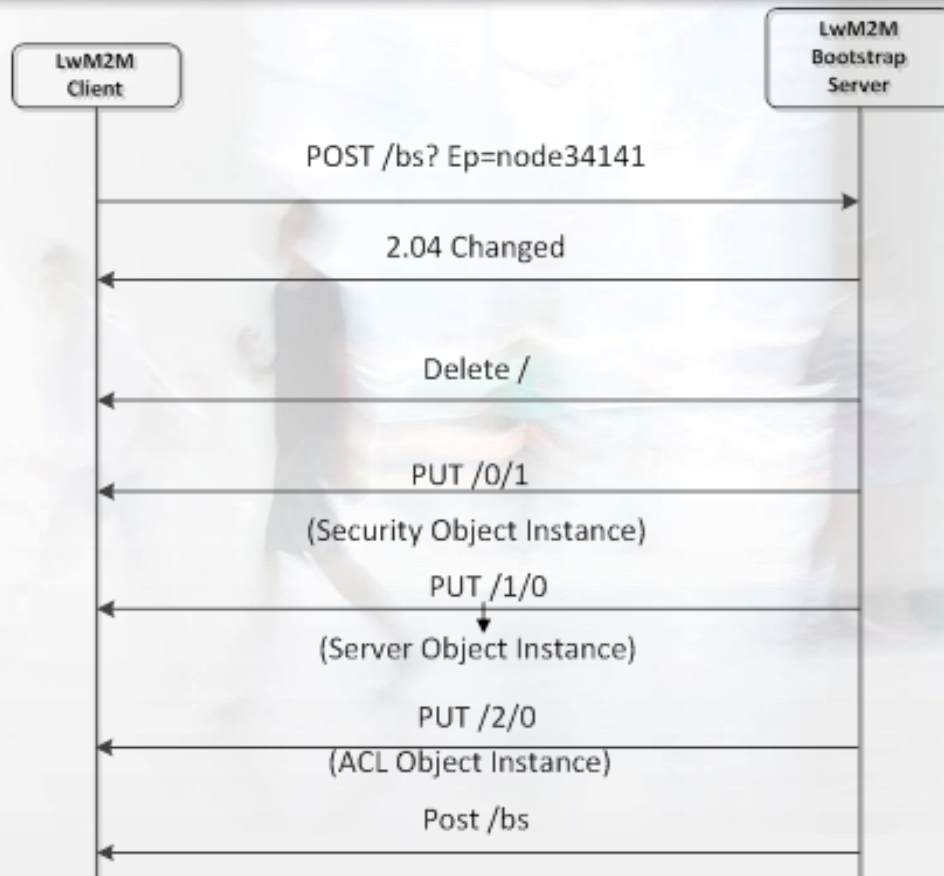


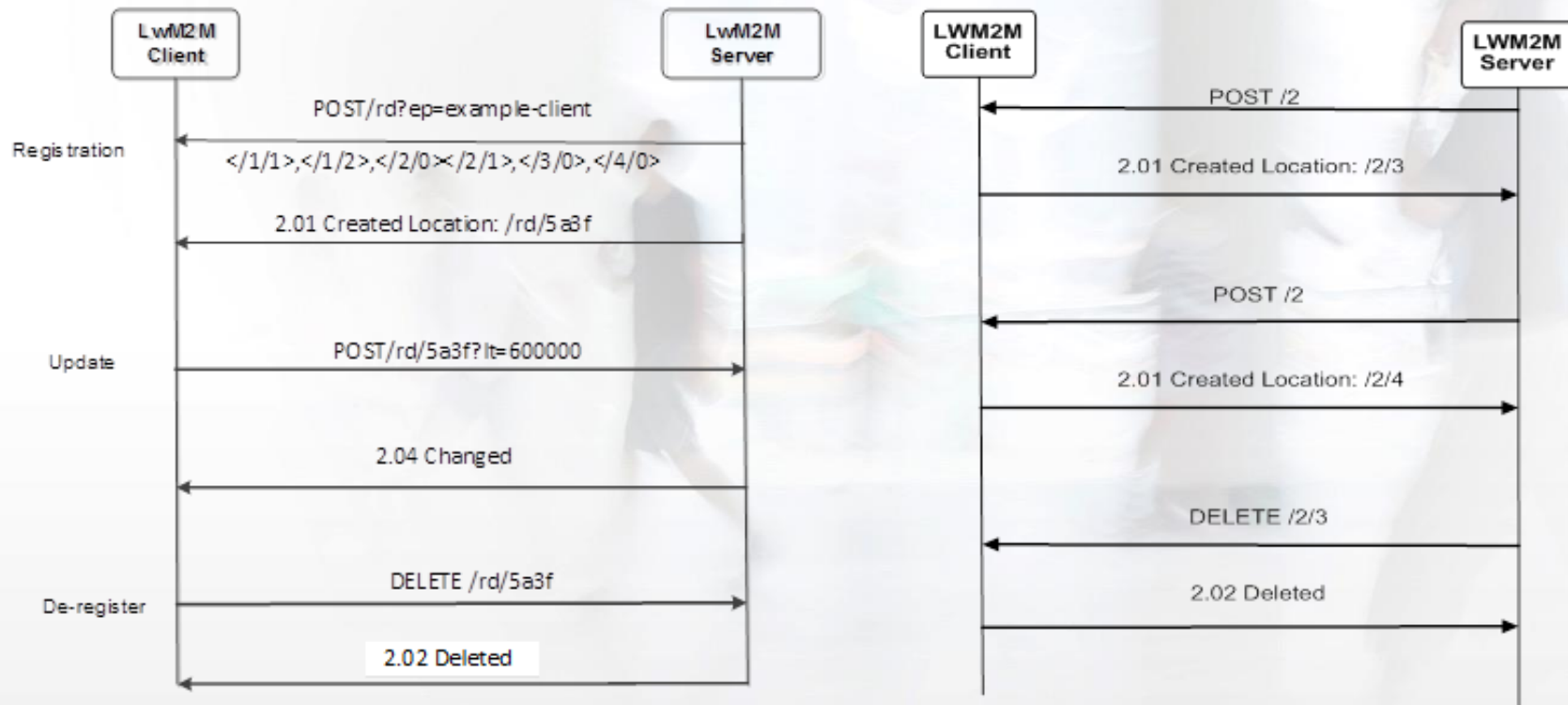
LwM2M can be used for both data plane (data reporting and devices actuations) and device management.

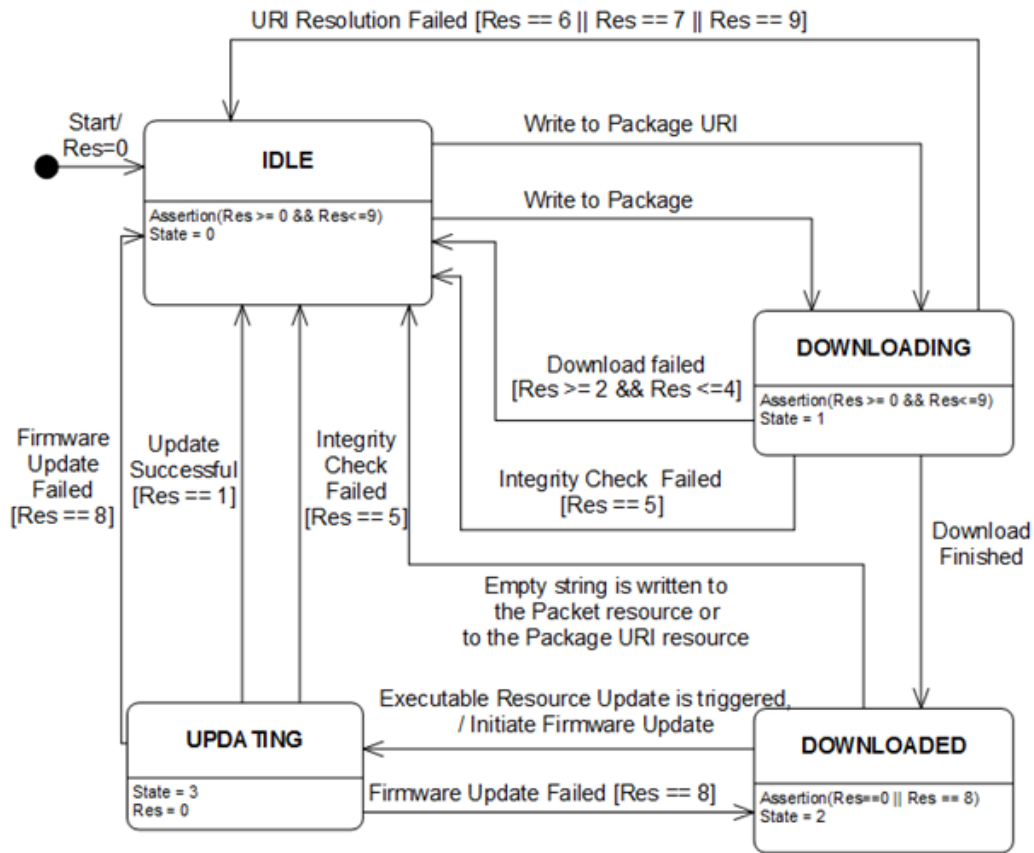
Strengths of LwM2M:

- LwM2M is a standard defined by OMA
- Adequate for both fixed and mobile devices
- Adequate for both data plane and device management
- Made for constrained devices (e.g < 20 kB RAM)
- Adequate for low powered battery devices thanks to low client footprint
- Minimizes bandwidth thanks to optimized bandwidth consumption, by definition of 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

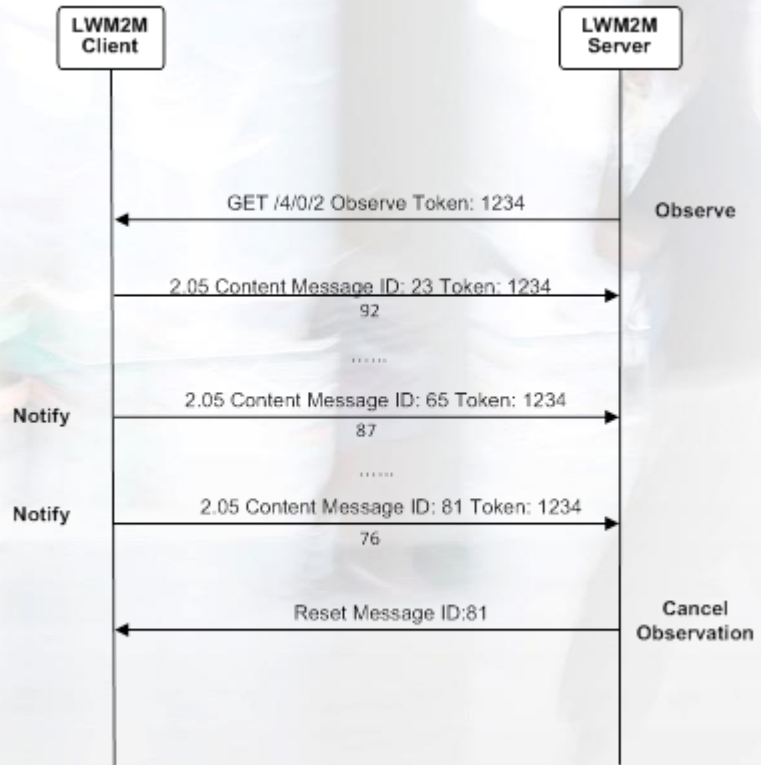






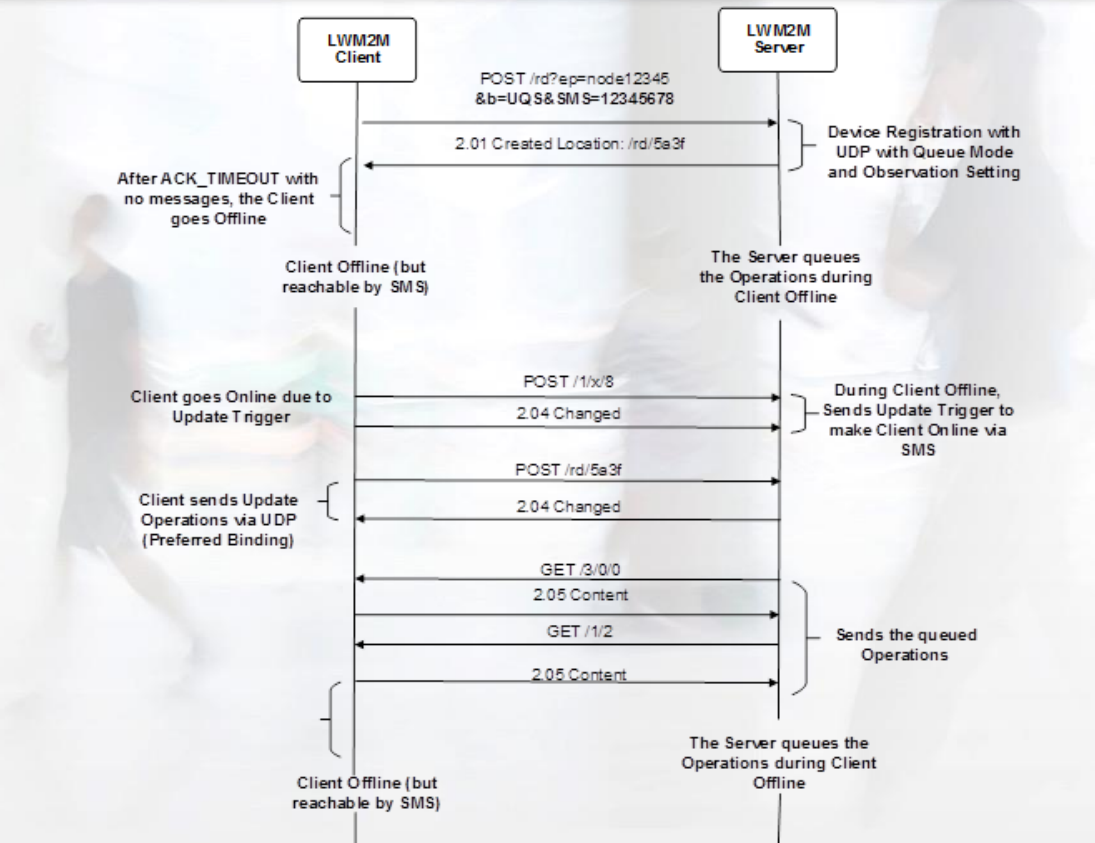


- Power sources and its values of the LwM2M Device
- Battery level of the LwM2M Device
- Memory status of the LwM2M Device
- Supported binding modes of the LwM2M Device
- Version of hardware/software of the LwM2M Device
- Capabilities of the LwM2M Device

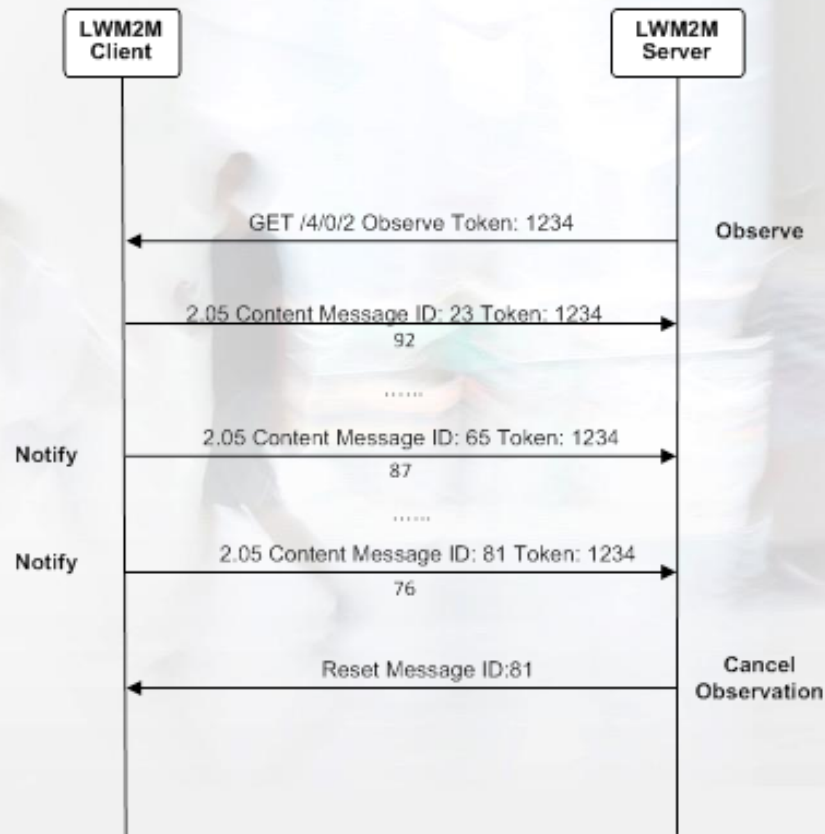


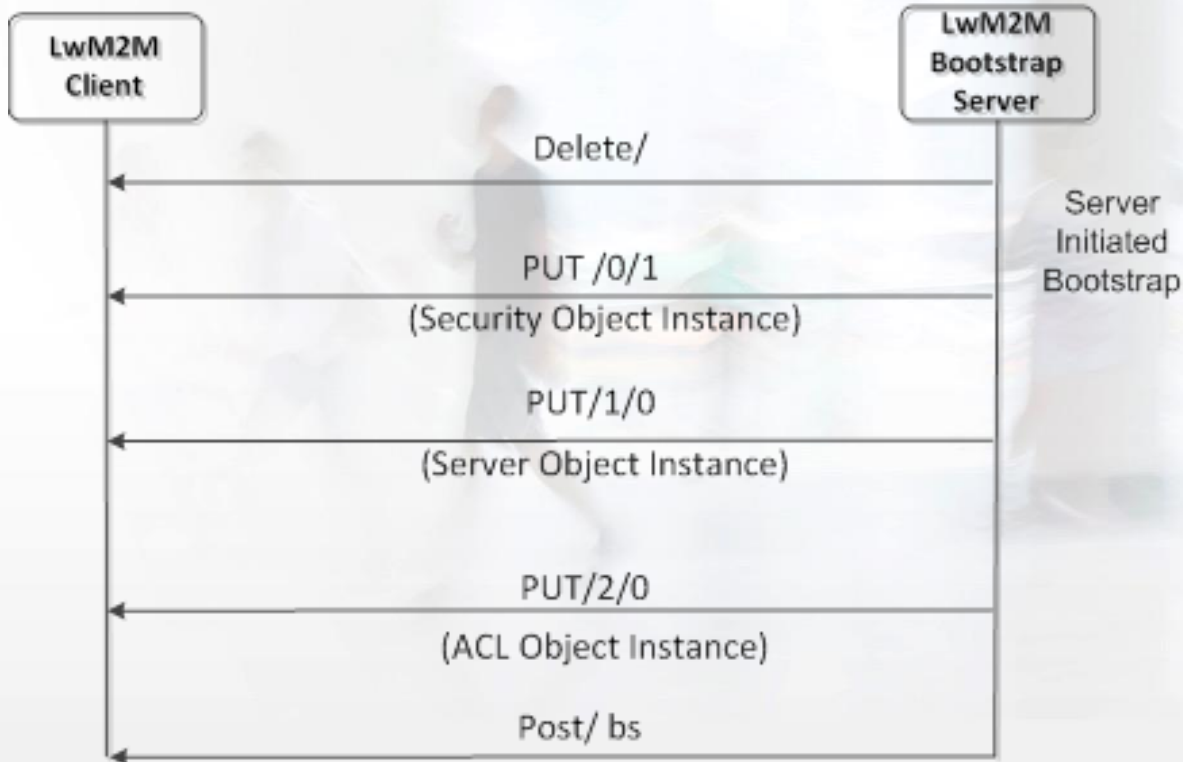
- Mapping of necessary Cellular and Wi-Fi technologies
- Managing basic parameters needed for those technologies functioning like APN, WEP keys etc.,
- Adding relevant parameters for bearer selection for cellular connectivity
- Security is covered by DTLS and relevant section provide multiple details

- Ability to setup access control on Objects for various LwM2M server
- 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



Example of Device Management & Service Enablement interface exchanges for Queue Mode with SMS Registration Update Trigger





Types of credential procedures supported

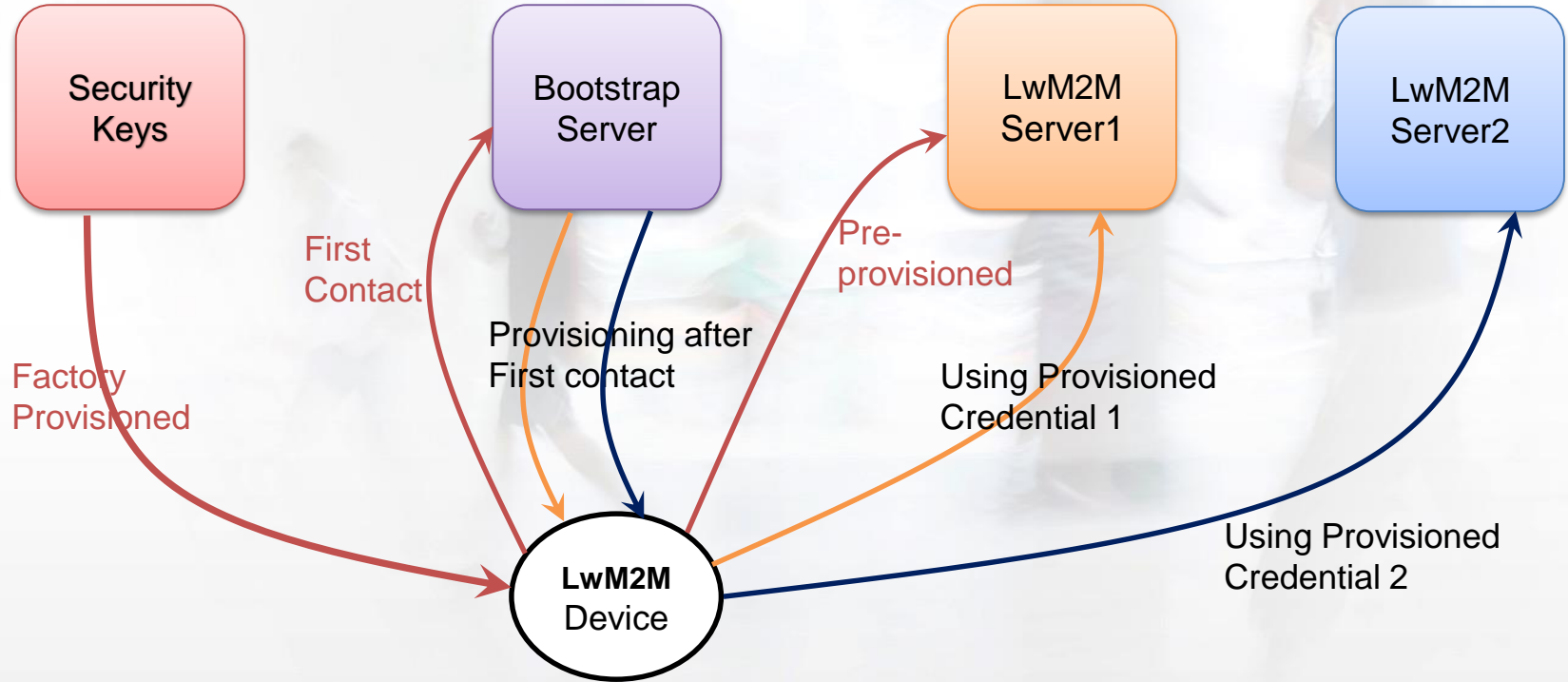
- Certificates
- Pre-shared key
- Public Raw Key

Security paths

- DTLS
- SMS
- DTLS over SMS

LwM2M Security abilities

- Initial keys can be replaced during bootstrap procedure
- Multiple servers could be added with different credentials
- Provide security in every path



- URI based approach for target identification
- Objects and resource classification
- Supports versioning of objects
- OMA, Organizations and private registrations possible
- OMNA has the collection of LwM2M Objects and Resources registry

- Simple resource model with the core set of objects and resources defined in this specification. The full list of registered objects can be found at [OMNA].
- 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.

- 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.



Thank You

[OMA HELP](#)