MARKETING REPORT

# MR-278
## Managing Machine-to-Machine Systems with CWMP

**Issue: 1**
**Issue Date: November 2015**

Issue History

| Issue Number | Approval Date | Publication Date | Issue Editor | Changes |
|---|---|---|---|---|
| 1 | 9 November 2015 | 13 November 2015 | Apostolos Papageorgiou, NEC<br><br>Sumit Singhal, Ericsson | Original |

Comments or questions about this Broadband Forum Marketing Report should be directed to help@broadband-forum.org.


| | | |
|---|---|---|
| **Editor** | Apostolos Papageorgiou | NEC |
| | Sumit Singhal | Ericsson |
| **Lead Editor** | Apostolos Papageorgiou | NEC |
| **Contributors** | Apostolos Papageorgiou | NEC |
| | Sumit Singhal | Ericsson |
| | Jason Walls | QA Café |
| | Ataru Kobayashi | NEC |
| | Lindsay Frost | NEC |


  

TABLE OF CONTENTS



  

## List of Figures



## List of Tables



  

**Executive Summary**

This Marketing Report describes current and ongoing enhancements of the CWMP protocol in the direction of managing Machine-to-Machine (M2M) systems, thus motivating and supporting the industry to employ CWMP in various scenarios that deviate from its traditional use.

M2M systems are developed in the context of domains such as industrial automation, facility management, e-health, logistics, agriculture, smart home, and more. The expected business value of such systems is huge and the management of the devices that participate in them often has different requirements than the management of standard CPEs (Customer Premises Equipment) such as routers or set-top boxes.

Among the M2M-specific requirements are generic management functions such as device grouping, concurrent device access, service switching etc., which are functions that have been addressed by recent CWMP enhancements. In addition to describing how to implement these functions using CWMP, this Marketing Report also provides analyses and examples of domain-specific CWMP M2M deployments.

  

# 1 Introduction

Machine-to-Machine (M2M) devices are devices that have a sensing, actuating, or any automated data-generating task that runs without human intervention and has connectivity to a network which aggregates and processes data from many sources. Any kind of sensor devices, smart meters, cameras, home devices, automation machines, but of course also computing devices like smartphones, all are M2M devices, if they are executing such a task. M2M systems, in turn, are those systems which are empowered by M2M devices, including an end-to-end platform for providing enhanced and homogenized access to the M2M data. As the enabler of the Internet of Things (IoT), M2M is expected to play a huge role in terms of technological importance and market size.

The Broadband Forum develops and maintains the CPE WAN Management Protocol (CWMP – also widely known as TR-069 [1]). CWMP is used for the remote management and configuration of customer devices (mainly internet gateways and the devices connected to them) from the operator premises. CWMP can be used for the management of M2M devices and the Broadband Forum continues enhancing this aspect of CWMP by working on various M2M-related aspects of the protocol. Figure 1 illustrates the traditional scope of CWMP and Figure 2 highlights upon it the CWMP enhancements and extensions that have either been added recently or are currently under development in order to make CWMP fully appropriate for M2M scenarios. Each of the four aspects listed in Figure 2 is explained in the following subsections.

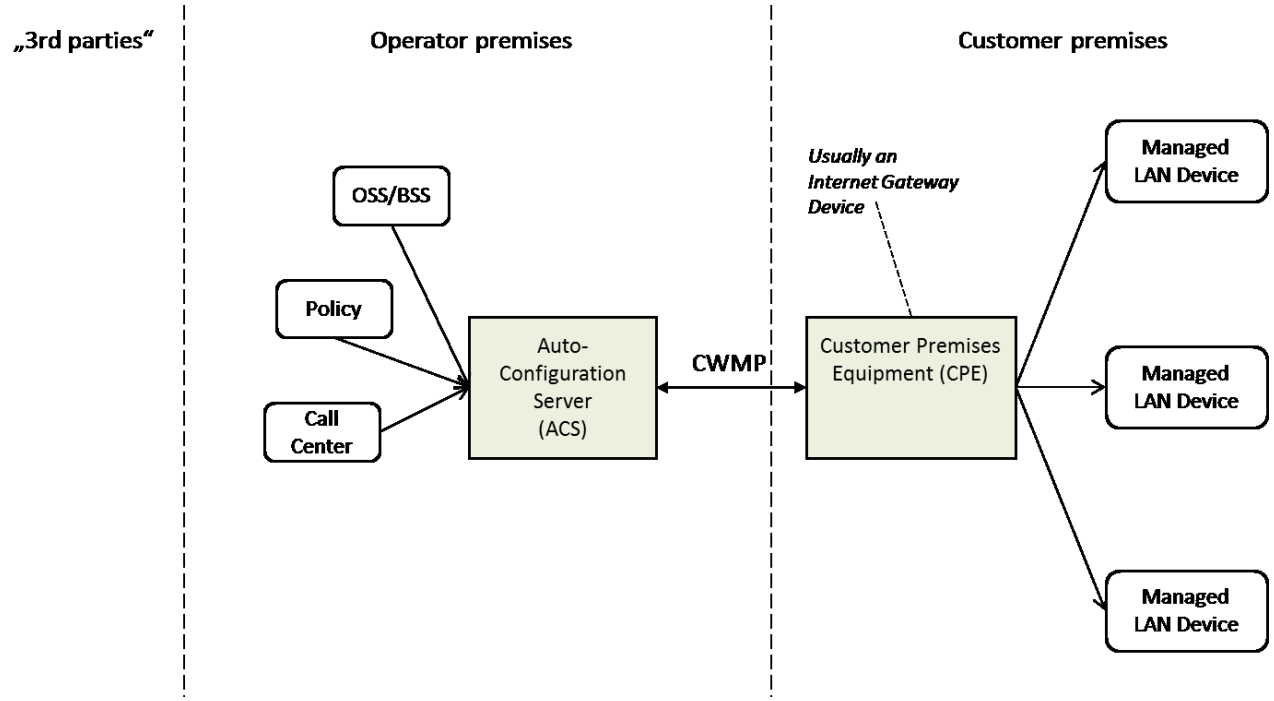


**Figure 1 – CWMP scope**

  

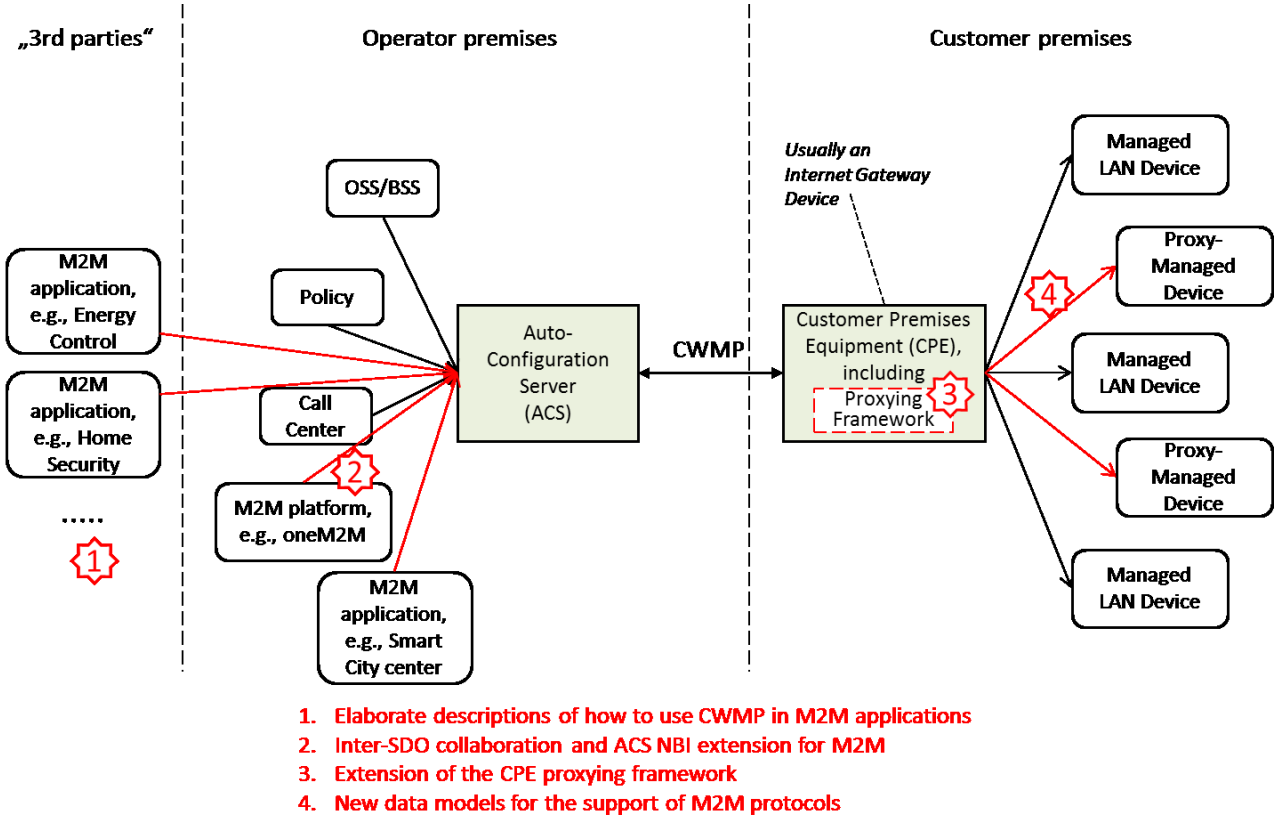


**Figure 2 – Recent and ongoing CWMP works supporting M2M solutions**

## 1.1 Elaborate descriptions of how to use CWMP in M2M applications

The Broadband Forum is working on detailed descriptions about how to manage M2M solutions using CWMP. The respective analyses have been performed in the context of internal Study Documents and some of the results are presented in Section 3 of this White Paper. The goal of this work is to support and promote the employment of CWMP in diverse M2M scenarios by providing analyses, implicit guidelines, and discussions about the technologies that are (or would be) involved in concrete CWMP-supported M2M applications. The focus is placed on generic functionalities that are common for different M2M applications, as well as on domain-specific details of important Use Cases.

## 1.2 Inter-SDO collaboration and ACS NBI extension for M2M

Through cooperation between the Broadband Forum and oneM2M, CWMP has already been included as one of the three main M2M management protocols in Release 1 ("aubergine") of oneM2M [2]. More details about CWMP usage inside oneM2M platforms can be found in the mentioned release.

The specific work done in oneM2M includes the usage of the CWMP protocol to fulfil the oneM2M management requirements. This includes:

  

- Protocol mapping between the oneM2M Service Layer and the Broadband Forum CWMP protocol.
- Mapping between the oneM2M management-related resources and the CWMP protocol RPCs (Remote Procedure Calls) and Device:2 data model defined in TR-181 issue 2 [3].
- Defining new Device:2 data model elements to fulfil oneM2M specific management requirements that cannot be mapped on existing resources.

The Broadband Forum is also continuously working on ensuring the compatibility of the entities involved in these two protocols, namely CWMP and oneM2M. For example, it is ensuring the compatibility of the ACS with the M2M Service Layer of the oneM2M service platform by adding M2M-related requirements and defining an M2M Profile in the ACS Northbound Interface (NBI) requirements document (TR-131a1 [4]).

## 1.3 Extension of the CPE proxying framework

The latest TR-069 specifications [1] include more and more features for the CWMP proxying mechanism and framework. More specifically, TR-069 has specified two proxying mechanisms, namely the EmbeddedDevice and the VirtualDevice mechanisms, which are being continuously extended in order to cover more challenging proxying features and use cases. Proxying is for obvious reasons extremely important for M2M scenarios, e.g., for enabling the CWMP-based management of UPnP- or ZigBee-based M2M devices.

## 1.4 New data models for the support of M2M protocols

The Broadband Forum is constantly adding data model elements for the support of more and more technologies at the customer premises. Many of the recently added data models are extremely important for M2M applications, e.g., the ZigBee-, UPnP-, and ETSI M2M data models, but also the Cellular Interface, the proxying-related objects, and various other parts.

  

# 2 Background and technical landscape

Although various M2M solutions might be developed based on cellular networks, i.e., by adding 3G or LTE capabilities to the involved M2M devices and letting them connect directly to a base station, many other M2M solutions would be rather provided with deployments that are based on M2M Gateways, i.e., gateways that reside close to the M2M devices and mediate the connectivity of the M2M devices to the backbone network. The M2M Gateways can, in turn, have either fixed or mobile access to the backbone network. Thus, both fixed and mobile network operators can have an important part in M2M systems, while there are various roles that they can have. This section gives a high-level view of M2M Gateway-based deployments, describes the potentially involved stakeholders (from a network operator perspective), and explains why CWMP can have a very important role in managing M2M Gateway-based systems.

## 2.1 Gateway-based M2M deployments

A very high level view of Gateway-based deployments is shown in Figure 3. In this scenario, M2M Gateways (e.g., residential gateways, building controllers, road-side units, industrial automation controllers, outdoor gateways, or public WiFi hotspots) monitor and control the M2M devices, potentially enforce some "network-edge intelligence", and connect the devices via a core network to backend systems (e.g., Cloud platforms and databases).

This kind of deployment might be preferred over cellular-based solutions because of reasons such as the following: (i) a gateway might be already in place, (ii) we might be interested only in devices that are in the range of a gateway, (iii) the devices might be cheaper without, e.g., LTE capabilities, (iv) the (potentially fixed-access) connection of the Gateway might offer higher bandwidth and reliability, and more. As already implied by the previously listed types of gateways, this deployment might be preferred for applications such as home automation, utilities management, industrial control, public safety and transport, whereas applications with higher device mobility such as logistics, fleet monitoring, etc. might prefer cellular-based solutions. For the connection of the Gateway itself to the core network, either fixed or cellular connections (or both at the same time) might be used. Using fixed and cellular access at the same time, with CWMP managing both uplinks, might make sense especially for critical services such as home security or metering, where redundancy is required.

  

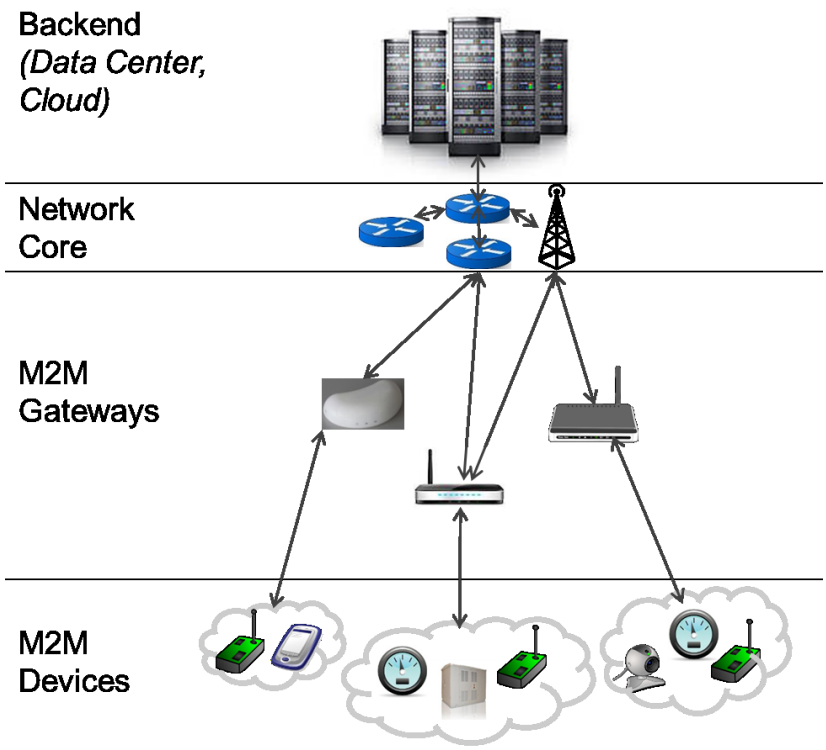


**Figure 3 – High-level view of Gateway-based M2M deployments**

## 2.2 M2M stakeholders and roles

A number of sub-sets of users of M2M services can be identified: consumers in the home, business users and facility managers, city governments, logistics businesses, energy providers, and more. Further, a large number of individual owners of "machines" may be drawn for the first time into such a business ecosystem. However, all these parties are summarized here as potential "Application Users", while the focus is put on the stakeholders that enable the operation of an M2M system from a technological point-of-view.

Figure 4 illustrates the major technical roles in the wide M2M ecosystem, while Figure 5 gives an overview of the roles that these stakeholders can potentially have. Each stakeholder can have one or more roles depending on her/his interests, e.g. a person can be both a "Device Owner" and an "Application User", while a network operator can provide simply the network access or provide the M2M platform and M2M applications, as well.

  

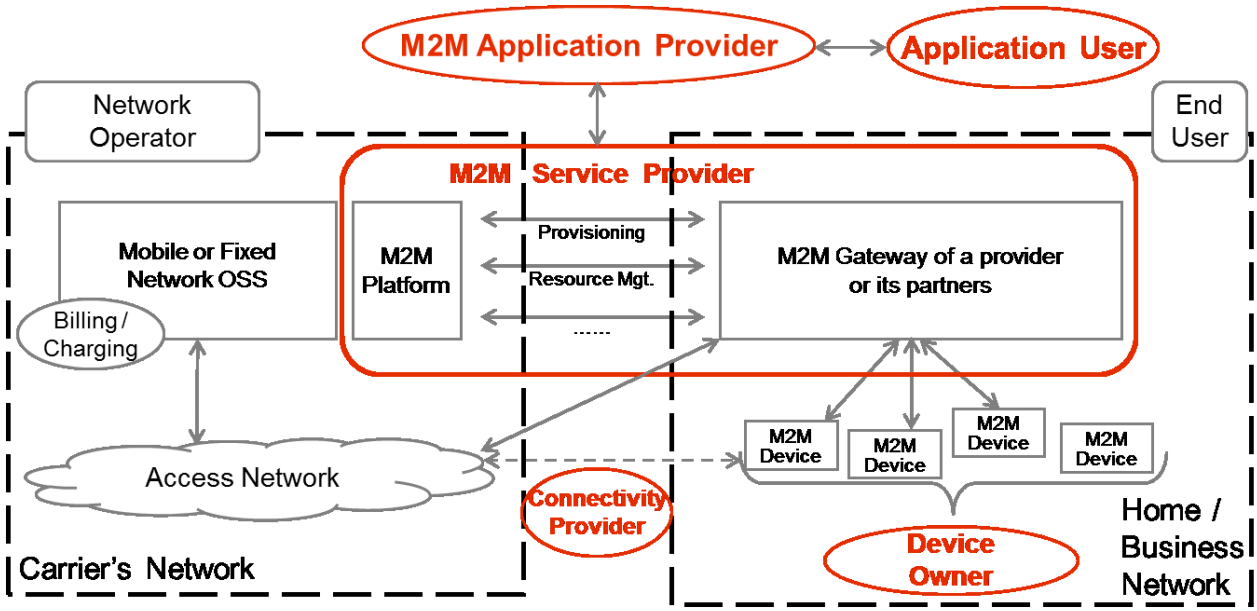


**Figure 4 – Roles in the M2M ecosystem**

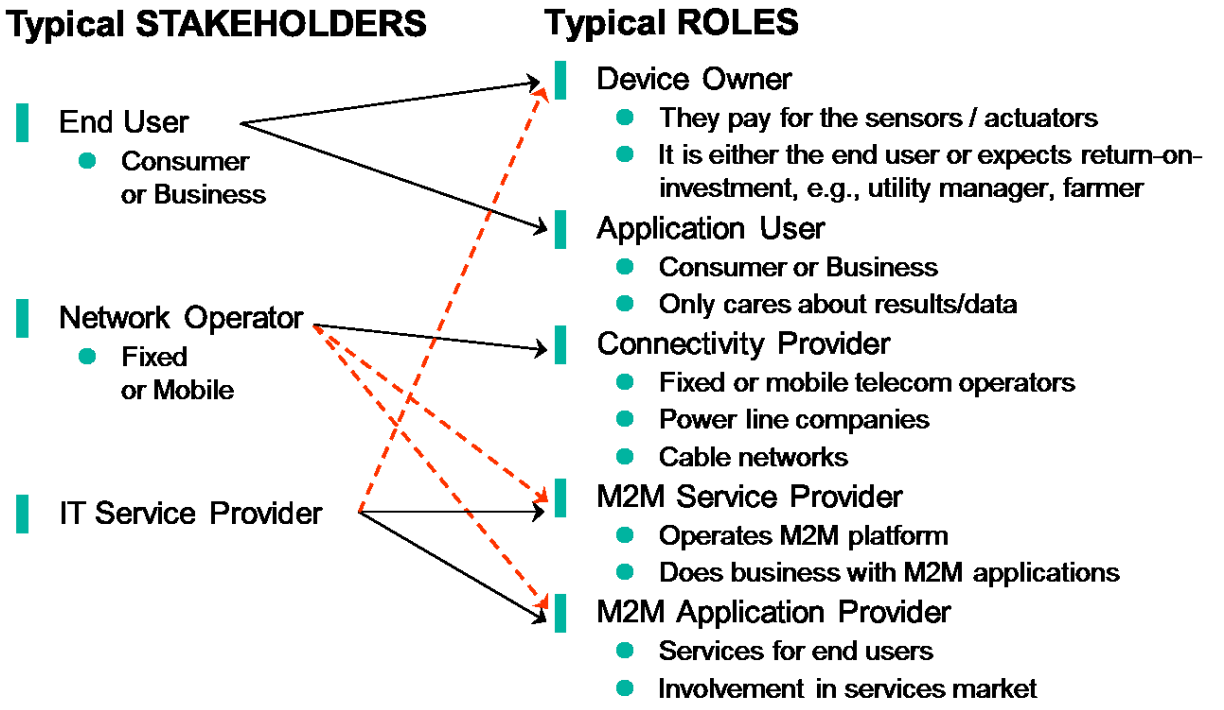


**Figure 5 – Potential roles of typical M2M stakeholders**
**(solid arrows show the main roles, while dashed arrows point to additional roles that a stakeholder might take over)**

## 2.3 The role of CWMP in M2M

The importance of CWMP for M2M systems becomes obvious because of the following characteristics:

- Firstly, Gateway-based M2M deployments (cf. Figure 3) have a very similar architecture with Home networks, which are the traditional scope of CWMP. This means that using CWMP in M2M systems would not require big efforts or costs, but rather simple adjustments of currently used CWMP ecosystems.
- Secondly, if network operators have multiple roles in the M2M ecosystem (cf. Figure 4), they might want to integrate their ACSs with their M2M platforms and manage M2M devices in the same way that they have been managing home devices, i.e., using CWMP.
- Thirdly, for many M2M Use Cases, M2M devices will be deployed into the existing home networks, which are already managed with CWMP, and will require the same basic functions, e.g., discovery, update, etc.

However, M2M systems have also differences to home networks, mainly in terms of the usage scenarios, the used access technologies, the requirements of the backend systems, and more. Therefore, as already explained in the introduction, CWMP has not always been equipped with all features and functions that are required for efficient management of M2M systems. Further, companies need guidance and domain-specific examples before they take the step of managing M2M with CWMP.

  

# 3 M2M usage scenarios for CWMP

In the introduction, we summarized four categories of M2M-related enhancements that the Broadband Forum has been performing on CWMP. This section describes various M2M usage scenarios of CWMP, providing case-by-case more concrete examples and references to these four categories of CWMP enhancements.

The M2M usage scenarios of CWMP can be divided into two categories. Firstly, there is a series of usage scenarios that correspond with generic functionalities which are commonly needed or might be typical for M2M systems in general. Secondly, there are various specific M2M domains which have their own requirements.

The following sections provide a description, as well as a list of enabling or related CWMP features and techniques, for various usage scenarios of both mentioned categories. Section 3.1 focuses on generic M2M management, while Section 3.2 focuses on domain-specific M2M management.

## 3.1 Generic M2M management

### 3.1.1 Device grouping

DESCRIPTION:

The concept of device grouping is very common in discussions about the Internet of Things or about the control of complex appliances. Defining groups, creating them, allowing automatic discovery of their properties, etc. are additional aspects, which are required in many practical implementations.

In the M2M area, it is common that several physical devices work together to provide an M2M service. In the example of Figure 6, the devices CAMERA, DOOR SENSOR, and WINDOW SENSOR work together to provide a home security service, while the devices CAMERA and MOTION SENSOR work together to provide a health care service. In this M2M scenario, an ACS might need to manage the devices that work together collectively, as a device group. However, the physical devices providing a service normally connect to only one ACS, so different physical devices of the same group might be primarily managed by different ACSs. This makes it challenging to manage the devices as a group.

  

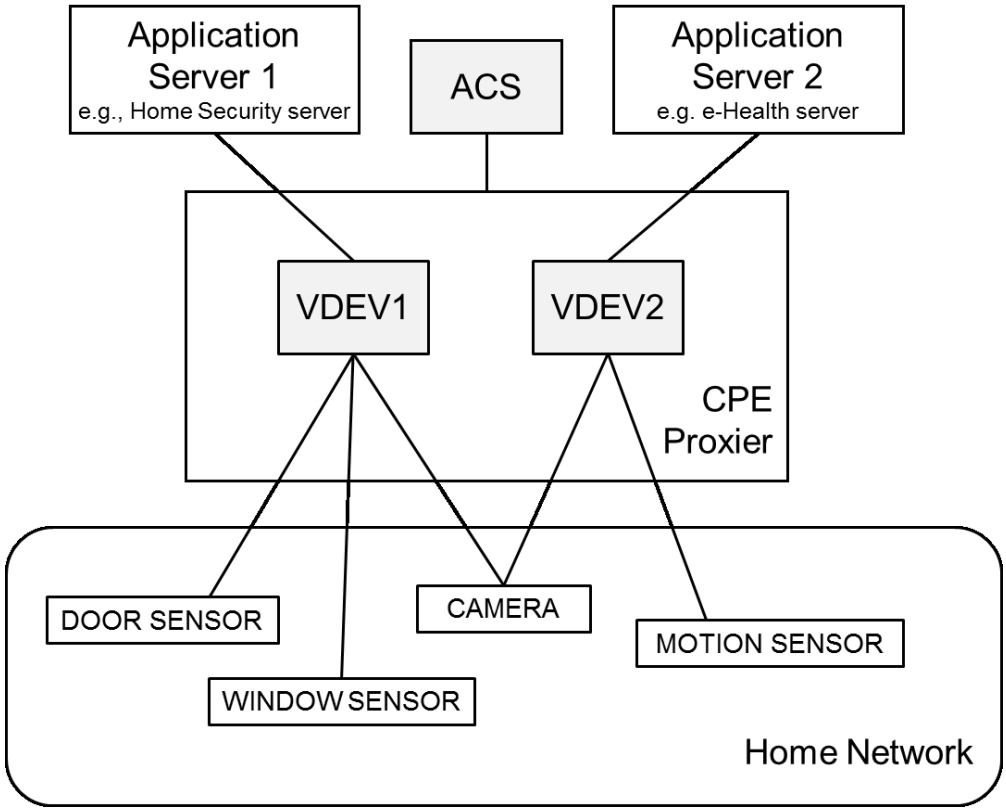


**Figure 6 – Grouping of managed M2M devices**

ENABLING OR RELATED CWMP FEATURES AND TECHNIQUES:

- The CPE Proxier can construct multiple virtual devices in order to ease the collective management of the proxied devices. A virtual device in this situation will represent a group of devices (rather than one device, as is the case in the traditional usage of TR-069 VirtualDevice objects). Each virtual device can then be managed by a different Application Server without conflicts. An Application Server is a server with ACS functionality which is employed by a specific application provider (and not necessarily a telecom operator) in order to manage devices or groups of devices that serve that particular application.
- In the example of Figure 6, there are two home network services, namely home security service and health care service. Therefore, a VirtualDevice VDEV1 is constructed from DOOR SENSOR, WINDOWS SENSOR, and CAMERA, while a VirtualDevice VDEV2 is constructed from CAMERA and MOTION SENSOR.
- In addition to the TR-069 proxying framework and especially the VirtualDevice mechanism, new M2M-related data models could also be exploited to support device grouping. In the ZigBee data model, for example, services are categorized based on an application profile, each application profile having a unique application identifier defined by the ZigBee Alliance. Using this information, the CPE Proxier could construct a virtual device for the physical devices providing the same service type.

  

### 3.1.2 Concurrent access

DESCRIPTION:

This usage scenario refers to the case when two ACS may manage the same device at the same time. This has been avoided in traditional home networks, but Figure 6 of the previous usage scenario ("Device grouping") gives already a very good example of why and when this might be useful in M2M solutions.

The same issue appears if an M2M device is logically partitioned in terms of management. This might be motivated by the fact that in an M2M ecosystem, new stakeholders are introduced that may access different levels of an M2M device (cf. Section 2.2). For example, an operator of a network may manage an M2M device on a low level, e.g., it may be allowed to update the firmware of the device. On the other hand, an M2M service provider might manage certain aspects of the M2M device at a higher level, for example, to configure parameters that are influencing the behavior of the application execution environment.

ENABLING OR RELATED CWMP FEATURES AND TECHNIQUES:

- Concurrent access can be implemented with virtual devices pointed at different ACSs (see previous usage scenario in Section 3.1.1).
- Alternatively, the ACS which a device is pointing to ("ACS URL" setting) can be frequently switched back and forth between the different ACSs during operation, whenever this is required.
- Finally, concurrent access can be achieved by calling the ACS Northbound Interface (NBI) API (Application Programming Interface) from alternate applications.

### 3.1.3 Service switching

DESCRIPTION:

This usage scenario assumes that an M2M device is accessible (but not necessarily manageable) by at least two independent M2M services in the Cloud and/or locally. Despite the similarity to the usage scenario of concurrent access (3.1.2), this scenario is completely different in that it does not require the device to be manageable by two ACSs. It simply requires that an ACS can dynamically re-configure the device in order to fulfill its tasks for one M2M service or another. Figure 7 makes this difference easier to understand, especially when compared with Figure 6 (which could be a case of concurrent access).

A webcam that can be configured to serve either a home application or a remote security system, an Internet Gateway Device that can be "turned into" an M2M Gateway on demand, or an e-health device that can switch configurations depending if it is used by its owner or by a doctor, are all examples for this usage scenario.

  

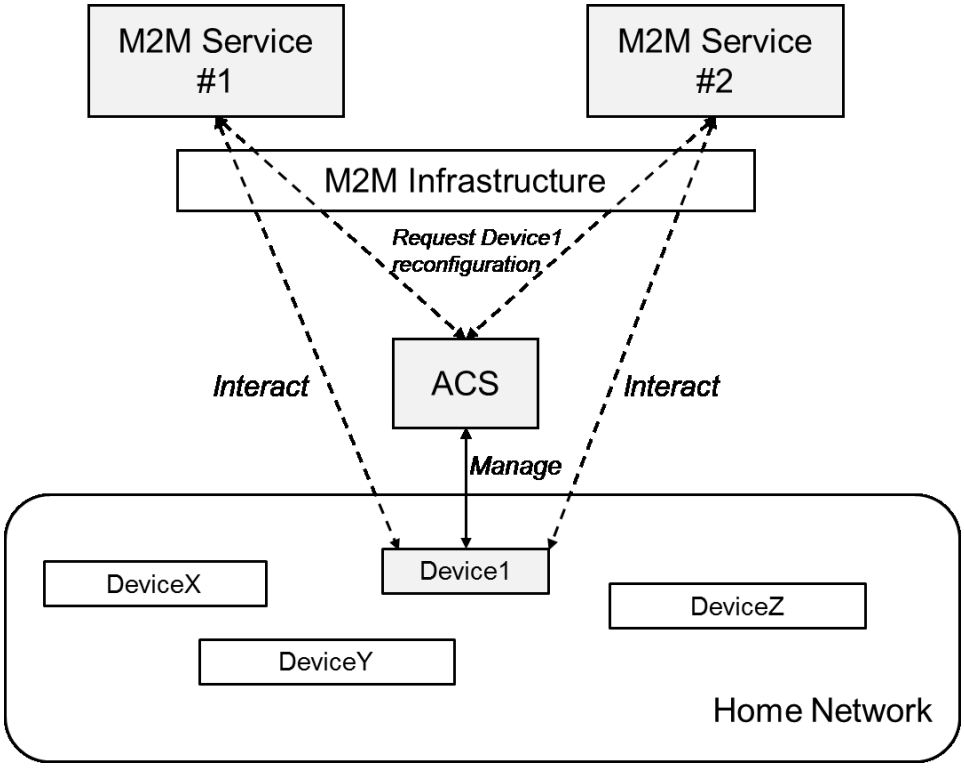


**Figure 7 – Service switching for an M2M device**

ENABLING OR RELATED CWMP FEATURES AND TECHNIQUES:

- Service re-establishment (resume control) with backup/restore, thus restoring the system to the state that best supports the currently required service.
- ACS-assisted firmware switching ("firmware download"), each time downloading the firmware that supports the currently required service.
- Software-level re-configuration by using the ExecutionEnvironment and SoftwareModules objects of the Device:2 data model.

### 3.1.4 Automatic service provisioning

DESCRIPTION:

This usage scenario refers to the support of zero-touch activation of M2M services that are enabled by M2M devices or M2M device modules purchased by the user. Assuming that the purchased devices are discoverable and the customer is unable to activate their services, then the operator can support this activation in an automated or semi-automated manner through a procedure such as the one described in the following (the numbering of the steps corresponds with the numbered actions of Figure 8):

1. The customer installs discoverable devices or devices that can discover other devices. After the installation, the devices are turned on and they start to send discovery and

  

advertisement messages. The M2M Gateway is able to capture these messages and extract metadata from them.

2. The extracted device metadata are stored as parameters so the ACS is informed about them and forwards them to a functional element called Service Locator (SLOC).
3. When SLOC receives the messages it will look into its database to find appropriate URLs that will point to Service Repositories (SREP) that contain software that once installed on the M2M Gateway will enable the desired service.
4. SREP returns to SLOC URLs pointing to the software modules that can be provisioned. This answer may also include additional information about resources needed in the home environment.
5. SLOC returns this information to the ACS. In order to select a service from multiple URLs, the ACS may either interact with the customer or perform automatic selection.
6. The ACS downloads the software module from the URL it received from the SLOC, e.g., from an FTP server.
7. The ACS delivers the fetched software module to the Execution Environment of the M2M Gateway.
8. The M2M Gateway sends a message to the device saying that the service is available on the M2M Gateway.
9. The device can interact with the M2M Gateway.

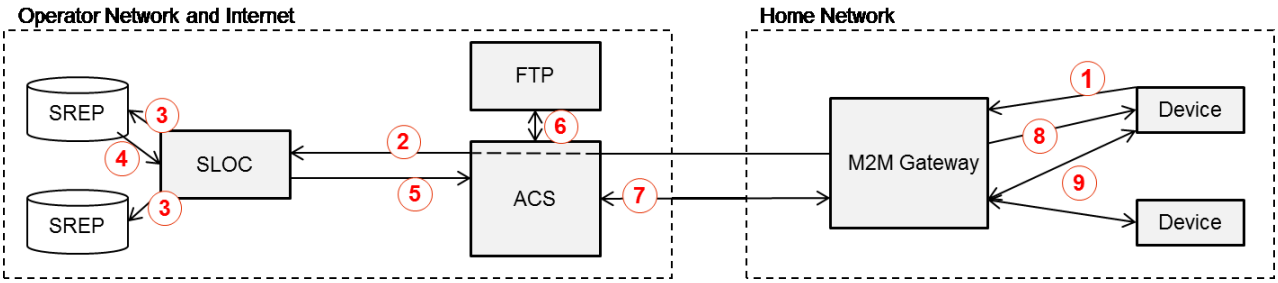


**Figure 8 – Service provisioning of dynamically installed M2M devices**

ENABLING OR RELATED CWMP FEATURES AND TECHNIQUES:

- Steps 6-9 of Figure 8 can be implemented in an obvious way based on the ExecutionEnvironment and SoftwareModules data models of TR-069.
- Recently completed data models for technologies used by discoverable and hot-deployable M2M devices (e.g., UPnP and ZigBee) increases the likelihood that described scenario is implemented in CWMP-managed systems.

### 3.1.5 Data filtering configuration

DESCRIPTION:

This usage scenario refers to the need for data management and filtering techniques that are required before data is reported from the M2M devices to the M2M platform or a similar backend system. The M2M Gateways that reside close to the data sources might do more with the actual M2M data than simply forwarding them, e.g., data filtering, aggregation, or pre-processing.

  

Network bandwidth limitations, system load, energy consumption, storage costs, or I/O bottlenecks are possible reasons for this.

Considering all these constraints, it makes sense to have a data filtering module on the M2M Gateway itself. This filtering module can help in determining which data needs to be reported to the M2M platform. The filtering module could include various filters, and be independent of any vertical domain or application. Now, this filtering module can be configured by an ACS as shown in Figure 9. Some important points related to the usage of the ACS-configurable Filtering Module are the following:

- The interface between a GW module and the M2M platform which is used to report the M2M Device data would be replaced by the interface of the Filtering Module. The Filtering Module might be still owned by the operator.
- The M2M Platform operator can configure the filtering module from the ACS to perform operations like:
    - (De-)activate data reduction/filtering techniques, e.g., “sampling”, “important points selection”, “aggregation”.
    - Adjust thresholds or settings (e.g., rates, importance levels) for the aforementioned filtering techniques.
    - Block data sources.
    - Prioritize certain applications or data over others.
    - Perform access control, e.g., by determining which (potentially third-party installed) GW modules are allowed to forward data to the backend at each moment, which data gets forwarded, and which of this data can be accessed by specific external application servers.

  

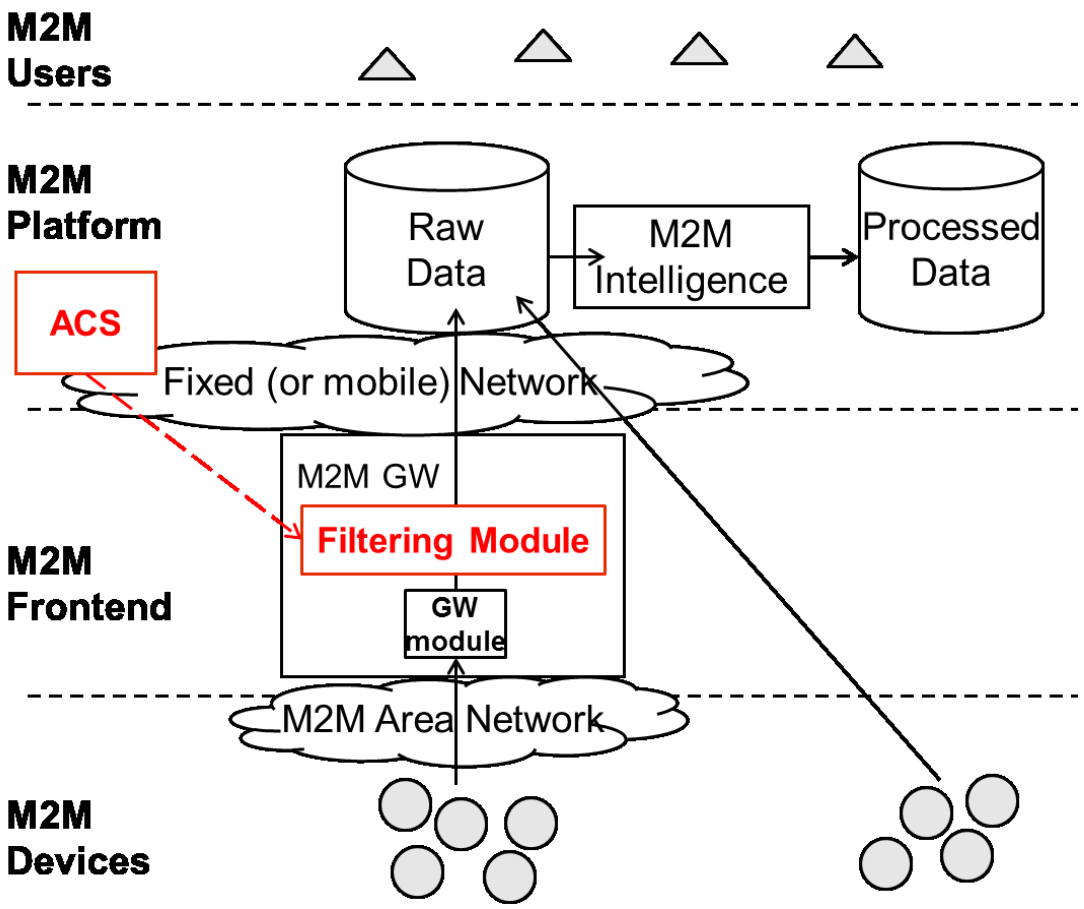


**Figure 9 – ACS-configurable M2M Data Filtering**

ENABLING OR RELATED CWMP FEATURES AND TECHNIQUES:

- For CPEs that include such a mechanism, an extension of Device:2 that models the ACS-configurable Filtering Module with parameters about all important filtering settings would be a sufficient solution.

### 3.1.6 ETSI M2M data model management

DESCRIPTION:

ETSI has defined an M2M functional architecture that incorporates the capability to utilize CWMP to perform management functions within its Remote Entity Management (REM) mechanisms. In the ETSI M2M Functional Architecture, the REM is responsible for the following management functions:

- General Management: retrieval of information related to the M2M Device or Gateway that hosts the ETSI M2M Service Capability Layer (SCL).
- Configuration Management: configuration of the M2M Device or Gateway's capabilities in order to support ETSI M2M Services and Applications.

  

- Diagnostics and Monitoring Management: diagnostic tests and retrieval or reception of alerts associated with the M2M Device or Gateway that hosts the SCL.
- Software Management: maintenance of software associated with the SCL and M2M services.
- Firmware Management: maintenance of firmware associated with the M2M Device or Gateway that hosts the SCL.
- Area Network Management: maintenance of devices on the M2M Area Network associated with the SCL.
- SCL Administration: administration capabilities in order to configure and maintain an SCL within the M2M Device or Gateway.

For these seven management functions, ETSI has defined a set of common data objects that are shared by CWMP data models.

ENABLING OR RELATED CWMP FEATURES AND TECHNIQUES:

- The CWMP data model includes objects and parameters for ETSI-defined resources. etsiMemory, etsiFirmware and etsiSoftware are among these resources and they can be accessed by using the "Device.DeviceInfo" object of the CWMP Data Model.
- Additionally, extensions have been defined for the ETSI resources etsiSclMo, etsiAreaNwkInfo and etsiAreaNwkDeviceInfo.
- The ETSI REM solution requires support for optional RPCs at the M2M Device or Gateway. These RPCs include, Upload, ScheduleDownload, ScheduleInform etc.

## 3.2 Domain-specific M2M management

As captured in previous sections, CWMP can be used to address multiple scenarios of M2M device management. This allows CWMP to be applied in existing and newer domains where traditionally alternate methods are used to achieve the same results. Stakeholders of specific M2M domains are looking for cost- and time-efficient solutions to maximize revenues of M2M systems and provide additional solutions and services. This renders CWMP an interesting choice for various domain-specific M2M deployments. Section 3.2.1 gives an overview of specific M2M domains which could profit by new features and supported technologies of CWMP, while Section 3.2.2 describes an example domain-specific CWMP M2M deployment in more detail.

### 3.2.1 Overview

Contrary to, e.g., home routers, which are traditionally managed by a single provider, i.e., the Internet Service Provider (ISP), many devices of new M2M domains might support the services of (and be managed by) two or more authorities or organizations. In such cases, CWMP features such as "multiple ACS support", "automatic service provisioning" and "service switching" (cf. Section 3.1) will be extremely important.

  

Table 1 helps to understand why a list of important M2M domains would profit by the aforementioned features. The variety of the involved stakeholders (each of them potentially operating their own ACS) and the variety of technologies which are often crucial for the respective M2M domain implies the important of the M2M-enabling CWMP features.

**Table 1 – M2M domains with multiple stakeholders which can exploit new CWMP features**

| **Domain-specific CWMP M2M Usage Scenarios** | ***Authorities involved, potentially requiring "management by multiple ACS", "automatic service provisioning", and/or "service switching"*** | ***Example relevant technologies, for which recently developed CWMP data models or domain-specific extensions can be used*** |
|---|---|---|
| Ambient-assisted living | Healthcare organization, sensor/actuator manufacturers, government | RFID, ZigBee, zwave, WiMAX… |
| Home energy management | Electricity provider, Telecom operator, Smart Grid stakeholders | ZigBee, OSGP, Smart meter protocols, … |
| Agricultural solutions | Farm owners, sensor/actuator manufacturers/owners | RFID, GPS, … |
| Surveillance systems | Smart City, police, security companies | IP, UPnP, WiFi, WiMAX… |
| Privacy solutions | Government, Telecom operator | … |
| Facility Management | Facility manager, Building owner, Telecom operator, Smart City | BACnet, Modbus, ZigBee, … |

### 3.2.2 Example deployment of a domain-specific CWMP-managed M2M system

Buildings of the future are expected to be monitored and controlled in a highly automated manner. TR-069 should consider the M2M technologies used and the peculiarities involved in such facility management scenarios because:

- Firstly, CWMP can be used for the remote management of CPEs in any kind of facility.
- Secondly, even simple residential buildings are expected to use automation systems and various M2M devices, including those initially designed for sophisticated facility management and energy control. Not only "building modules", but even "in-home devices" can be involved in these systems.

In bigger facilities, M2M gateways are deployed to configure, control, and aggregate the data from existing ICT (Information and Communications Technology) infrastructures like building automation systems, occupancy systems, surveillance systems, local weather stations, remote weather forecasts, security systems, etc. Many of the above, e.g., security systems or occupancy detectors, as well as smart metering devices, are relevant for residential buildings already. Accordingly, many protocols and standards from the buildings and smart energy domains come into play, which have not been relevant for traditional Use Cases of home ICT systems.

One of the reasons why TR-069 could play a big role in this story is the fact that although large energy and facility companies are extremely interested in the operation of in-home M2M devices, they can practically rarely install, own, or control them themselves. However, such devices can

  

help them enhance the tasks and the decisions of their central systems. Some examples from the energy domain would include: energy flow control according to weather conditions and facility usage and occupancy patterns, efficient preparation of resources, intelligent utilization of renewable energy sources (e.g., local use vs. feed-in), intelligent utilization of building storage (e.g. thermal storage), load balancing of electricity demand and local supply according to dynamic electricity pricing, and more.

The following main stakeholders are involved:

- *Holistic Management Service Provider*: A company that provides holistic management services for energy, material, and resource flows for any kinds of facilities. The actor provides the synergetic analytics over all data sources within different dimensions like time, space and context (including for example tariffs or waste-management fees), and provides decision support for advanced facility control operations. This actor is closely linked with the facility operator in order to provide holistic data management and control.
- *Facility Operator*: A company that is in charge of the operation of facility. The main focus is the main facility's metering and control system (e.g. building automation systems) and therefore the operation of the facility in a cost- and energy-efficient manner while complying with comfort, safety and environmental regulations. This actor will cooperate with third party facility services in order to enable holistic data integration. It is in charge of the business relations for all actors active within and for the facility, and to ensure compliance with privacy and confidentiality rules. In some cases the Facility Operator may be the same company as the Holistic Management Service Provider.
- *Third Party Facility ICT provider*: A company which provides an additional sensor/ control/ metering system into the facility operated independently from the main facility monitoring system (installed permanently or temporarily). This actor might have a business relation with the facility operator, and enables access to its sensed data with the M2M gateways for the purpose of the optimal facility operation.
- *M2M Service Provider*: A company that provides M2M services including entities like gateway, platform and enables the communication between them. The M2M Service Provider also exposes APIs for the development of all kinds of applications. The M2M Service Provider can expose different service levels to enable integrated data aggregation with different access rules. The M2M services provider provides communication means with local as well as remote infrastructure covering mobile and fixed access to facility internal as well as external data services and ICT systems.
- *Home/Building Owner*: A person that owns the building and is entitled to install any kind of M2M device, to which she/he can, in turn, provide access for any of the aforementioned stakeholders.

Figure 10 illustrates the overlapping of interests and responsibilities, as well as the variety of M2M protocols that can become relevant in the facility management usage scenario. For example, the protocol BACnet is very common for building automation, similarly to KNX and LonWorks, while Building Information Models (BIM), as well as Smart Grid-related standards can also become relevant. The telecom operator (or any other ACS operator) could then benefit from the ability to remotely configure these devices either in the interest of the Home Owner or in the interest of any other involved -and authorized- stakeholder.

  

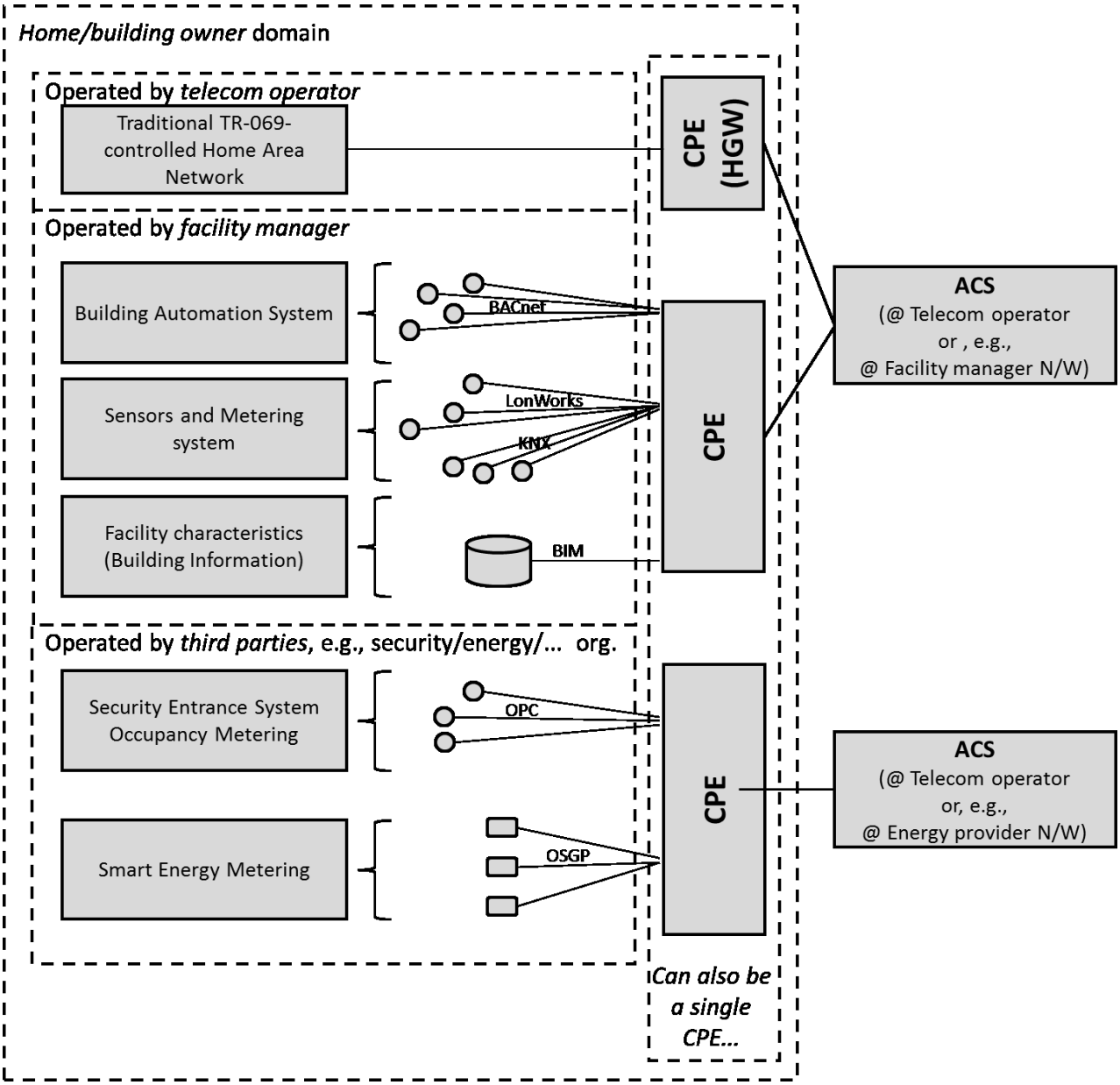


**Figure 10 – Typical deployment and responsibilities for the facility management usage scenario**

  

# 4 Terminology

## 4.1 References

The following references are of relevance to this Marketing Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Marketing Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.

A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

| Document | Title | Source | Year |
|---|---|---|---|
| [1] TR-069 | *TR-069 Amendment 5, CPE WAN Management Protocol* | Broadband Forum | 2013 |
| [2] oneM2M specs | *oneM2M published specifications* | oneM2M | 2015 |
| [3] TR-181 | *TR-181i2 Amendment 10, Device Data Model for TR-069* | Broadband Forum | 2015 |
| [4] TR-131a1 | *TR-131 Amendment 1, ACS Northbound Interface Requirements* | Broadband Forum | 2015 |

## 4.2 Definitions

The following terminology is used throughout this Marketing Report.

**ACS** Auto-Configuration Server. This is a component in the broadband network responsible for auto-configuration of the CPE for advanced services.

**CPE** Customer Premises Equipment; refers to any TR-069-enabled [1] device and therefore covers Residential Gateways, LAN-side End Devices, and other Network Infrastructure Devices.

**CWMP** CPE WAN Management Protocol. Defined in TR-069 [1], CWMP is a communication protocol between an ACS and CPE that defines a mechanism for secure auto-configuration of a CPE and other CPE management functions in a common framework.

  

## 4.3 Abbreviations

This Marketing Report uses the following abbreviations:

| | |
|---|---|
| **ACS** | Auto-Configuration Server |
| **API** | Application Programming Interface |
| **BACnet** | Building Automation and Control network |
| **CPE** | Customer Premises Equipment |
| **CWMP** | CPE WAN Management Protocol |
| **ETSI** | European Telecommunications Standards Institute |
| **FTP** | File Transfer Protocol |
| **GW** | Gateway |
| **ICT** | Information and Communications Technology |
| **IoT** | Internet of Things |
| **IP** | Internet Protocol |
| **ISP** | Internet Service Provider |
| **IT** | Information Technology |
| **LAN** | Local Area Network |
| **LTE** | Long Term Evolution |
| **M2M** | Machine-To-Machine |
| **MR** | Marketing Report |
| **NBI** | Northbound Interface |
| **OSS/BSS** | Operations Support Systems / Business Support Systems |
| **REM** | Remote Entity Management |
| **RFID** | Radio-frequency identification |
| **RPC** | Remote Procedure Call |
| **SCL** | Service Capability Layer |
| **SDO** | Standards Development Organization |
| **SLOC** | Service Locator |
| **SREP** | Service Repository |
| **TR** | Technical Report |
| **UPnP** | Universal Plug and Play |
| **URL** | Uniform Resource Locator |
| **WAN** | Wide Area Network |

  

**Notice**

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Broadband Forum Marketing Report has been approved by members of the Forum. This Broadband Forum Marketing Report is not binding on the Broadband Forum, any of its members, or any developer or service provider. This Broadband Forum Marketing Report is subject to change, but only with approval of members of the Forum. This Marketing Report is copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Marketing Report may be copyrighted by Broadband Forum members.

THIS SPECIFICATION IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS SPECIFICATION.

Broadband Forum Marketing Reports may be copied, downloaded, stored on a server or otherwise re-distributed in their entirety only, and may not be modified without the advance written permission of the Broadband Forum.

The text of this notice must be included in all copies of this Broadband Forum Marketing Report.

End of Broadband Forum Marketing Report MR-278

  