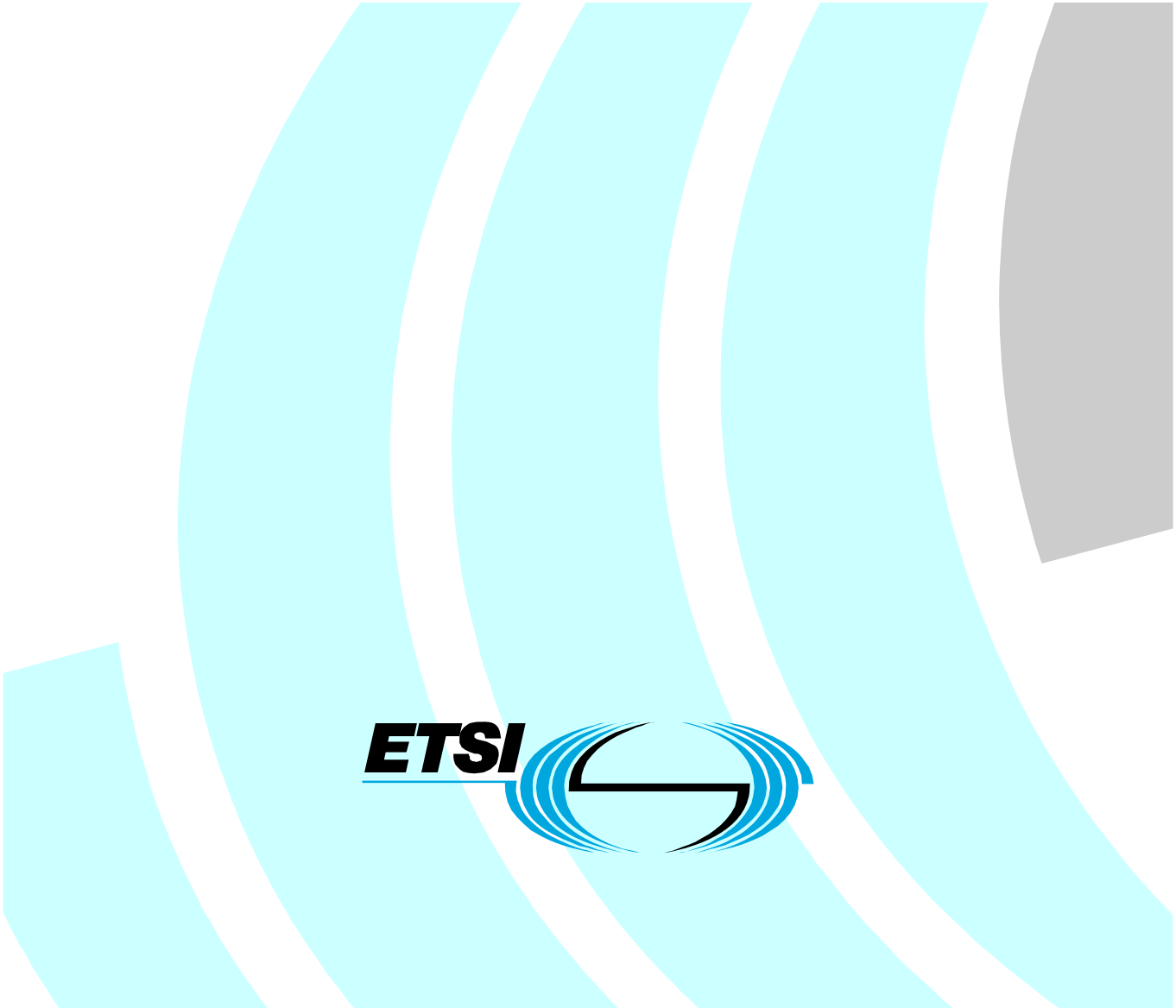
ETSI TR 102 691 V1.1.1 (2010-05)

Technical Report

Machine-to-Machine communications (M2M); Smart Metering Use Cases



Reference
DTR/M2M-00003

Keywords
interworking, M2M, smart meter, use case

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Machine-to-Machine communications (M2M).

1 Scope

The present document collects the Use Cases which have been identified for the Smart Metering M2M application. These Use Cases will identify actors and information flows, and will form the basis of future requirements work at TC M2M on Smart Metering.

Several parts of the present document have been taken from "Smart Metering Functionality Use Cases" [i.4] in particular the subclauses "General Use Case Description", "Scenario" and "Information Exchanges" of clause 5.2.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references,only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] European Commission Standardisation Mandate M/441: "Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability".

NOTE: Available at: http://www.cen.eu/cen/Sectors/Sectors/Measurement/Documents/M441.pdf

[i.2] Smart meters co-ordination group, final report (Version 0.7, 2009-12-10): "Standardization mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability M/441".

NOTE 1: http://www.cen.eu/cen/Sectors/Sectors/Measurement/Smart%20meters/Pages/default.aspx.

NOTE 2: Available at: http://docbox.etsi.org/M2M/M441/open_space/SMCG%20Meeting%20Docs/SMCG%20reports/V0.7_SM_CG_FinalReport_2009_12_10.pdf.

[i.3] Directive 2006/32/EC of the European Parliament and of the Council of 5 April 2006 on energy end-use efficiency and energy services and repealing Council Directive 93/76/EEC, published in the Official Journal of the European Union as OJ L 114 of 27.4.2006.

NOTE: Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:114:0064:0064:EN:PDF.

[i.4] ESMIG Document ESMCR003-002-1.0 (October 2009): "Smart Metering Functionality Use Cases", Engage Consulting Limited (assigned by ESMIG).

NOTE: Available at: http://docbox.etsi.org/M2M/M2M/20-Info/reference_documents.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

concentrator: acts as a network and protocol converter between the two transport technologies

NOTE: Obviously, it contains some others features that will be mentioned in the architecture document. The concentrator may have a multi utility role, in order to be able to handle meters managed by different kind of energy utilities.

Home "equipment(s)": On purpose, it is a generic wording that includes, in one or several boxes, the following functions (non exhaustive list):

- Modem for xDSL, GPRS or any other Wide Area network
- Residential/Home Gateway
- Home Service Gateway or/and Multi-Utility concentrator

Numerous domestic appliances could also be connected to the HAN. A PC or/and a displaying device is connected to the HAN.

local network: any less-than-1km-range technology is possible, wired or wireless (some examples could be Zigbee, M-Bus, Wireless M-Bus, PLC, etc.)

NOTE: Star or meshed network is possible.

operators: potential users for a specific use case from any of these different roles (utility provider / distributor, SM provider, Network Operator, etc.)

Smart Metering Information System: generic name that gathers several roles: service provider, energy supplier, energy distributor, network operator

NOTE: The exact content of this SM Information System and their physical implementation is out of scope of the Use Cases document.

use case: system descriptions from the user point of view

NOTE: They treat the system as a black box, and the interactions with the system, including system responses, are perceived as from outside the system. Use cases typically avoid technical jargon, preferring instead the language of the end user or domain expert.

The present document on hand lists and defines **system use cases**, which are normally described at the system functionality level (for example, create voucher) and specify the function or the service system provides for the user. A system use case will describe *what* the actor achieves interacting with the system. For this reason it is recommended that a system use case specification begin with a verb (e.g., *create* voucher, *select* payments, *exclude* payment, *cancel* voucher). Generally, the actor could be a human user or another system interacting with the system being defined.

A brief use case consists of a few sentences summarizing the use case.

Use cases should not be confused with the features/requirements of the system under consideration. A use case may be related to one or more features/requirements, a feature/requirement may be related to one or more use cases.

Wide Area Network (WAN): long range technology that enables exchanging data between parts of the Smart Metering Information System and the Concentrator

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

HAN	Home Area Network
M2M	Machine-to-Machine (communications)
TR	Technical Report
WAN	Wide Area Network

4 M2M application for Smart Metering

4.1 General description and reference to EC Mandate M/441

Following the European Commission Standardisation Mandate M/441, Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability, Smart Metering is defined as follows:

The general objective of this mandate is to create European standards that will enable interoperability of utility meters (water, gas, electricity, heat**), which can then improve the means by which customers' awareness of actual consumption can be raised in order to allow timely adaptation to their demands (commonly referred to as 'Smart Metering').**

Smart Metering primarily targets improvement of energy end-use efficiency as defined by Directive 2006/32/EC [i.3], thus contributing to the reduction of primary energy consumption, to the mitigation of CO2 and other greenhouse gas emissions.

According to article 13 "Metering and informative billing of energy consumption" of this directive states that competitively priced individual Smart Meters (also mentioned as Utility Meters) shall accurately reflect final consumers' actual energy consumption and shall provide information on actual time of use, in so far as it is technically possible, financially reasonable and proportionate in relation to potential energy savings.

Smart meters are utility meters (electricity, gas, water, heat meters) which may bring about the end of estimated bills and meter readings, and provide customers and energy distributors and suppliers with accurate information on the amount of utility being used.

Smart Metering provides:

- Customers with the information they require to become energy savvy and make smarter decisions about their energy usage,
- Energy suppliers with the means to better understand and service their customers,
- Distributors with an effective tool to better monitor and manage their networks.

In addition, Smart Metering enables those customers who choose to generate their own electricity (*micro generators*) to be financially rewarded for their contribution to the national grid and distributors to better manage this contribution.

The report of the Smart Metering Co-ordination Group [i.2] documents a list of functionalities that are suggested to be provided by the Smart Metering Information Systems. This list does not include the metrological functions currently performed by conventional meters/metering systems which may also be taken into account.

The functionalities are grouped into 6 categories and are referred to in the remaining of the present document as Additional Functionalities.

For the purposes of identifying where new standards might be required, this clause describes the Additional Functionalities at a high level. Clause 5.2 provides a further detailed use cases specific description confirming that the scope of each functionality was properly defined.

The proposed list of 6 main "Additional Functionalities" are expressed in broad terms, so that they can be related to electricity, gas, heating/cooling (hereafter 'heat') and water. However, not all use cases listed in clause 5.2 have to be derived from these "Additional Functionalities".

F1 Remote reading of metrological register(s) and provision to designated market organisation(s)
General definition:
Metering system capability to provide at a distance the designated market organisation(s) with the value of the meter register(s) through a standard interface at a pre-defined time schedule or on request.

Explanation:
a) Meter readings and other metrological data recorded at the customer's premises, which are made available to designated market organisation(s) at a pre-defined time schedule and on request.
b) Includes export metering (i.e. provision of consumption and injection data and on net flows exported).

F2 Two-way communication between the metering system and designated market organisation(s)
General definition:
Capability of the metering system to retrieve at a distance data on e.g. usage, network and supply quality, events, network or meter status and non-metrological data and to make this data available to the designated market organisation(s).
Ability of the designated market organisation(s) to configure the metering system at a distance and to carry out firmware/software upgrades.
Ability of the metering system to receive information - for example information sent from the **Energy Services Provider** (and/or via relevant third parties e.g. distribution system operator or metering operator) to the end user customer.

Explanation:
a) Metering system to designated market organisation(s)
Uploading of data and information to permit e.g. monitoring of supply quality, outages (electricity), network leakage detection (water)
and identification of possible meter malfunction
- tamper and fraud detection
- diagnostics (mainly for electronic components)
- meter/metering system status (e.g. battery condition credit/prepayment mode)
  Also identification of incorrectly sized or blocked meters (water).

b) Designated market organisation(s) to metering system
Downloading data to metering system to enable e.g.:
- remote configuration of the meter or parameters used by the meter/metering system
- clock synchronisation
- software and firmware updates

c) Designated market organisation(s) to customer i.e. where messages/information shown on metering system.
Ability of the metering system to receive messages from designated market organisation(s), both standard and ad hoc, e.g. on planned interruptions, messages on price changes)
and to receive information (incl. account information).

F3 Meter supporting advanced tariffing and payment systems
General definition:
Support for payment systems:
Capability of the metering system to allow the customer to prepay for usage by suitable payment means, to connect a supply and disconnect it after a predetermined consumption or certain time duration.
Support for tariffing:
Metering system provided with multiple rate registers for consumption (and where applicable) injection to allow e.g. for time of use tariffs, critical peak, real-time pricing or combinations of these.

Explanation:
a) Prepayment
Metering system to support prepayment (and other payment) options
May also permit credit/prepayment switching

b) Multiple rate tariffs
Use of multiple registers within meter or recording of interval reads

F4 Meter allowing remote disablement and enablement of supply
General definition:
Capability of the metering system to allow the designated market organisation(s) at a distance to safely control or configure supply limitation (not gas), enable and disable supply through configurable parameters set at the meter.

Explanation:
Remote connection / disconnection and Remote flow/power limitation

F5 Communicating with (and where appropriate directly controlling) individual devices within the home/building
General definition:
Capability of the metering system to securely exchange data with home and building or energy management systems and where appropriate with individual devices within the home/building (e.g. air conditioners, heaters, boilers).

Explanation:
a) Used by the distribution **network operator** AND/OR **the Energy Services Provider** for remote load management applications
- by means of a local energy management system or home/building control system
- where appropriate by direct control of individual devices within the home/building

b) Used by **consumer** for remote control of individual devices

c) Used by customer for information on individual appliance consumption
information from microgeneration device(s) on gross electricity generated

F6 Meter providing information via portal/gateway to an in-home/building display or auxiliary equipment
General definition:
Capability of the metering system to provide information on total usage, injection and other metrological and non-metrological data for external visual display.

Explanation:
Interfacing with home communications systems / home area network
Enables meter to export metrological and other information for display and potential analysis.
Potential for home and building control applications and sophisticated energy management systems.
[In-home/building displays may also be preferable for information noted above]

These "Additional Functionalities" serve as a basis or frame for defining corresponding Use Cases for the Mandate M/441 [i.1], from which potential requirements can be derived for the Smart Metering System (see clause 5.2).

4.2 Example of a typical Smart Metering configuration

An example of a Smart Metering Information System contains Smart Metering devices (e.g. valves, electricity meter, gas meter, water meter,…) which are connected to a data centre via a communications gateway (figure 4.1).

The Data Centre collects data from the Smart Meter devices and is able to control relevant Smart Meter devices remotely via the communications gateway.

In this configuration example the gateway also provides an interface to Home Automation devices like sensors, displays and appliances and to electricity micro generators.

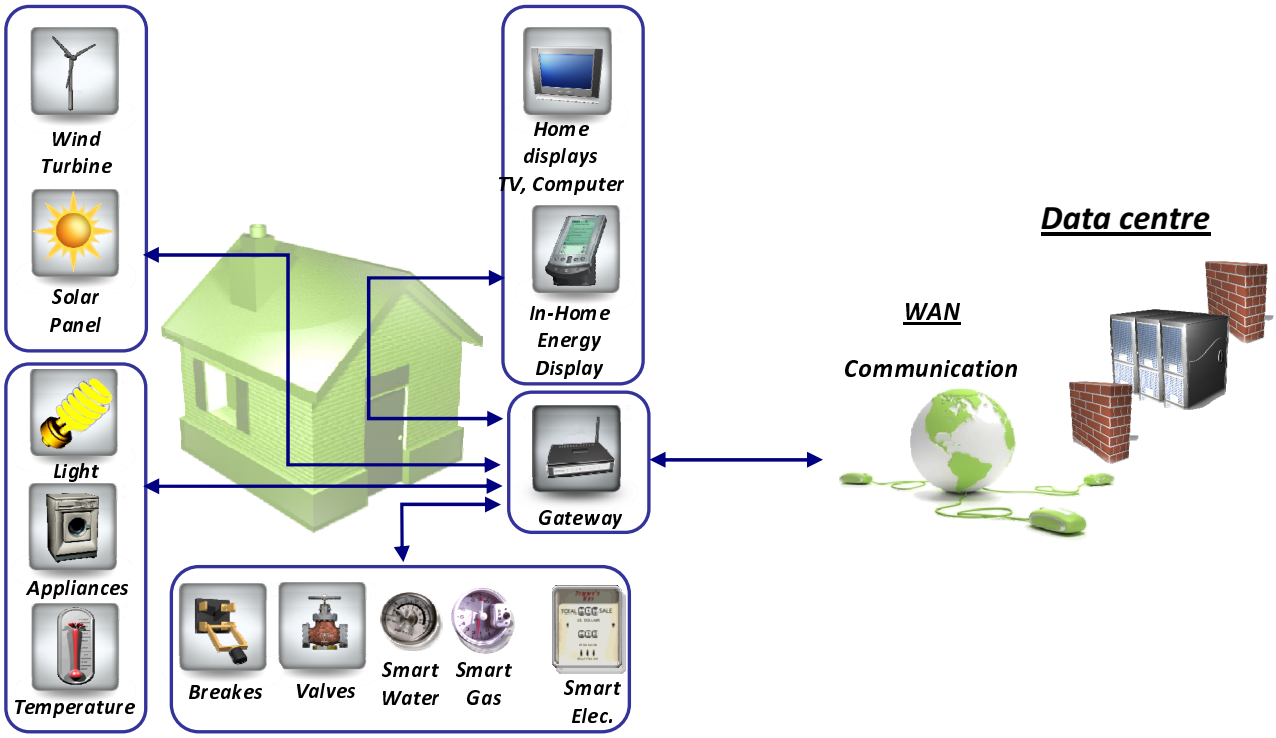


Figure 4.1: Typical Smart Metering Configuration

5 Smart Metering Use Cases

5.1 Overview

Use Cases according to definition in clause 3.1 will describe a system from the user point of view, describing what the actor achieves interacting with the system. Use Cases are used for deriving requirements on the system. For this purpose each Use Case described in the clause 5.2 starting with clause 5.2.3 is documented in the same way by using the same structure.

Only those new Use Cases shall be included in further revisions of the present document, which can be used as a justification of requirements not already justified by other - already included - Use Cases. The following template shall be used for adding further Use Cases without taking over the editor notes, which should serve in the template only as a help for describing the Use Case:

TEMPLATE

5.2.x.1 General Use Case Description

NOTE: Describe objective/goals of this use case in a high level but clear terms and list major issues that are highlighted.

5.2.x.2 Stakeholders

NOTE: In this clause, a set of definitions for who or what the Use Case is referring to. For example, consumer, network operator, database, bill entity, etc.

5.2.x.3 Scenario Case Description

NOTE: In this clause, descriptive text of the Use Case is provided showing how the stakeholders use the system. Describe detailed stepwise description.

5.2.x.4 Information Exchanges

NOTE: In this clause, definitions are provided for any information flows such as registration, data retrieval, or data delivery implied by the Use Case. Provide description for each type of information flow. For example, Meter - Read Data Recipient information flow (with attributes such as critical/non-critical data flow).

5.2.x.5 Potential new requirements

5.2.x.6 Use case source

5.2 Detailed Use Cases

5.2.1 List of Use Cases

This clause provides the list of use cases, which are described in detail in the next clauses and with that serve as a short overview.

List of Use Cases:

- Obtain Meter Reading Data
- Install, Configure & Maintain the Smart Metering Information System
- Support Prepayment Functionality
- Monitor Power Quality Data
- Manage Outage Data
- Facilitate Demand Response Actions
- Facilitate Distributed Generation Actions
- Manage the Distribution Network using Smart Metering Information System Data
- Manage Interference and Malfunctions to the Smart Metering Information System
- Manage Tariff Settings on the Smart Metering Information System
- Enable & Disable the Smart Metering Information System
- Interact with Devices at the Premise
- Manage Efficiency Measures at the Premise using Smart Metering Information System Data
- Display Messages

5.2.2 Use Cases Actors

This clause describes all actors involved in the Use Cases of the following clauses and which are listed here as Use Case stakeholders.

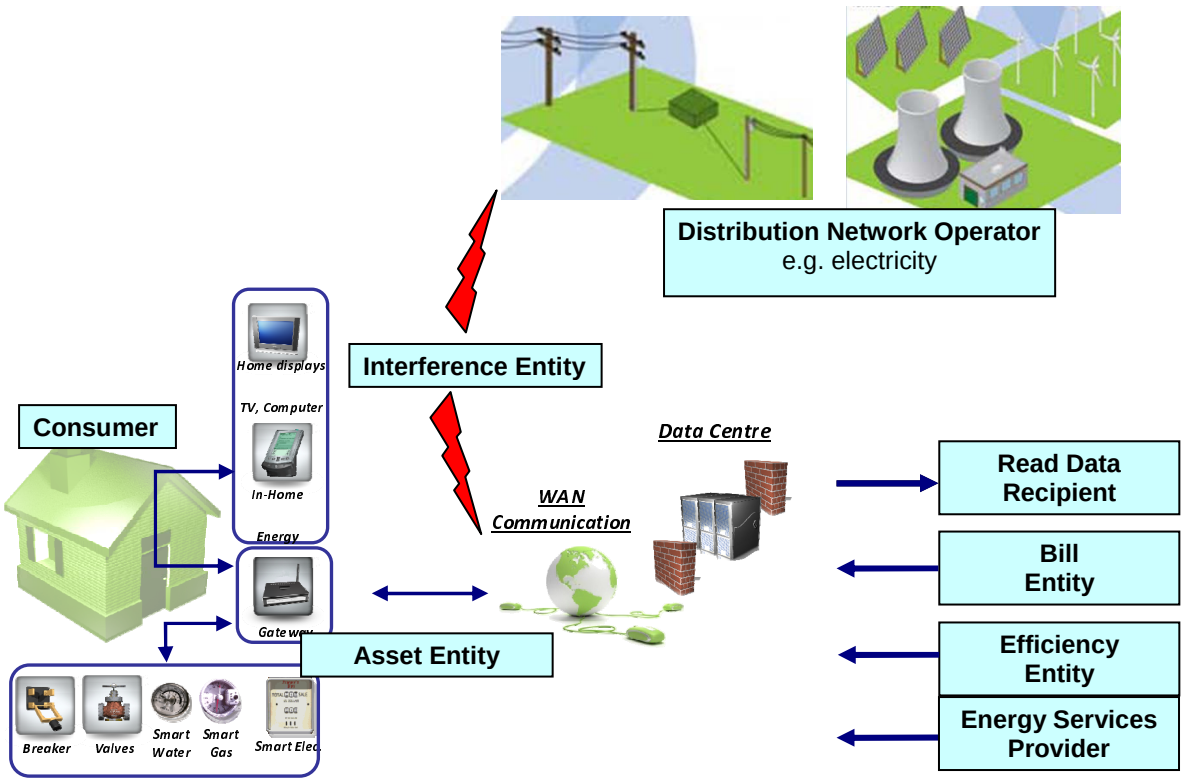


Figure 5.1: Actors of a Smart Metering Information System

Actor Name	Actor Role Description
Asset Entity:	Organization responsible for the installation, configuration and maintenance of the Smart Metering Information System assets (e.g. meters communication devices, SM gateway). As stated in the definition of the Smart Metering Information System there are several roles including respective responsibilities gathered. The allocation of installation responsibility to those roles is out of the scope of the Use Cases document on hand. The term "Asset Entity" is used in the document as the role of an actor of the Smart Metering Information System, who expects defined system responses interacting with the system during installation, configuration and maintenance. It could also be the case, that this role is split between the responsible parties listed in the definition of the Smart Metering Information System in clause 3.1
Bill Entity:	Organization responsible for billing the Consumer(s)
Consumer:	Organization or person consuming the electricity, gas, heat or water at the premise. The Consumer may also be the organization or person contracted with the Bill Entity to pay the bill
Efficiency Entity:	Organization or person providing efficiency measures advice to the Consumer(s)
Distribution Network Operator:	Organization responsible for managing the network of electricity, gas, heat and/or water provision to the premise
Read Data Recipient:	Organization or person authorized to receive meter reading data from the Smart Metering Information System. This actor can be any of the other actors defined in the scope that is authorized to receive read data
Interference Entity:	An individual or individuals who attempt to interfere with and/or defraud the Smart Metering Information System and/or the supply
Energy Services Provider:	Organization that offers energy related services to the consumer

5.2.3 Obtain Meter Reading Data

5.2.3.1 General Use Case Description

This High Level Use Case is aligned to the "Additional Functionality" F1 and F2 described in clause 4.1.
The Smart Metering Information System measures and records consumption of units and provides these in the form of readings. This Use Case describes how the Smart Metering Information System provides this meter reading data to the Read Data Recipient. This reading data may be routinely sent to the Read Data Recipient as per a defined schedule and an example of this would be periodic readings, interval values or load profiles.
It further describes how the Read Data Recipient can request and obtain meter reading data on demand from the Smart Metering Information System - as an example, where a reading is required to assist with resolving a billing query.

5.2.3.2 Stakeholders

Read Data Recipient

5.2.3.3 Scenario

Pre Conditions:

The Smart Metering Information System recognises the Read Data Recipient and has an address or addresses for them.

The Smart Metering Information System is installed and configured with a schedule to provide meter readings.
Meter reading data is available.

Post Conditions:

Meter reading data has been provided to the Read Data Recipient.
The Read Data Recipient is aware when a failure has occurred.

Trigger:

The meter's read reporting schedule has reached its allotted time to submit its readings or the Read Data Recipient decides that it needs to request meter reading data from the Smart Metering Information System.

5.2.3.4 Information Exchanges

Basic Flow:

1) For automatically scheduled readings:
    a) Smart Metering Information System registers meter reading along with time/date stamp
    b) Smart Metering Information System sends meter reading data to Read Data Recipient
2) For requested meter readings:
    a) The Read Data Recipient requests meter read data from the Smart Metering Information System
    b) The Smart Metering Information System validates the request
    c) The Smart Metering Information System sends the meter read data to the Read Data Recipient

Alternative Flow:

1) Smart Metering Information System fails to:
    - register meter reading along with time/date stamp; or
    - record meter reading data in its memory; or
    - send meter reading data to Read Data Recipient; or
    - validate the request to obtain meter readings.

2) Smart Metering Information System records error type with time/date stamp in its memory

3) Smart Metering Information System sends error notification to Read Data Recipient

5.2.3.5 Potential new requirements

- On demand readings with minimal time delay for distribution network management applications such as overload or outage detection.
- The M2M System should support accurate and secure time synchronisation. M2M Devices and M2M Gateways may support time synchronization or secure time synchronisation.
- M2M Application should be able to specify a periodic reporting of specific parameters for a specific M2M Device or group of M2M Devices. The M2M Application should be able to modify the value of the requested time period.
  In addition to the periodic reporting mechanism, M2M Application should be able to request the same report to the same M2M Device or group of M2M Devices in an on-demand mode.
- The M2M System should support transaction handling between cooperating objects capable of handling this functionality.
- The M2M System should support the following mechanisms for receiving information from M2M Devices and M2M Gateways:
  - Receiving unsolicited information (passive retrieval).
  - Receiving scheduled information.
  - Operating particular algorithms for retrieving information (e.g., round robin, random within given time window, round robin groups with random reply in given time window).
- The M2M System should be able to authenticate the M2M Device or M2M Gateway. For M2M Devices supporting authentication and connected via an M2M Gateway, the authentication may be performed directly to the M2M System or to the authenticated M2M Gateway.
- When there is a request for data or device access, the M2M Device or M2M Gateway should be able to authenticate the M2M Service Capabilities or M2M Applications from which request is received:
- The M2M System should support a security solution that makes it impossible to acquire information about the data collected by eavesdropping at any point in the network. A particular application may or may not require the use of such security solution. Security solution should not prevent regulatory requirements such as lawful interception.
- End points of the M2M System should be able to verify the integrity of the data exchanged.

5.2.3.6 Use case source

ESMIG, Document: Smart Metering Functionality Use Cases, ESMCR003-002-1.0, October 2009 [i.4].

5.2.4 Install, Configure & Maintain the Smart Metering Information System

5.2.4.1 General Use Case Description

This High Level Use Case is aligned to the "Additional Functionality" F2 described in clause 4.1.
It describes how the Asset Entity installs, configures and maintains the Smart Metering Information System as required.
It describes how the Asset Entity undertakes these configuration and/or maintenance actions where an issue on the Smart Metering Information System has been recognised.
The Use Case also describes the monitoring and upgrade of the Smart Metering Information System's functionalities by the Asset Entity (including firmware updates).

5.2.4.2 Stakeholders

Asset Entity, Consumer.

5.2.4.3 Scenario

Pre Conditions:

The Smart Metering Information System is available for installation, configuration or maintenance. The Smart Metering Information System recognises the Asset Entity and has an address for them.

Post Conditions:

The Smart Metering Information System confirms to the Asset Entity that the installation, configuration or maintenance action has been completed.
The Asset Entity is aware when a failure has occurred.

Trigger:

The Asset Entity identifies that there is a need to carry out an installation, configuration or maintenance action on the Smart Metering Information System.

5.2.4.4 Information Exchanges

Install Basic Flow:

1) The Asset Entity arranges to visit the Consumer's premise at a pre-arranged time with the relevant stock of metering equipment.

2) The Asset Entity representative visits the Consumer's premise at the pre-arranged time and installs for first time or replaces the existing metering equipment with the Smart Metering Information System.

3) The Smart Metering Information System, once installed, contacts the Asset Entity to self-register in their systems.

4) The Smart Metering Information System informs the Asset Entity of any required information at start up (e.g. meter readings, meter technical information, etc.) and requests any updates if required.

5) The installation is complete.

Configure Basic Flow:

1) The Asset Entity sends configuration settings to the Smart Metering Information System.

2) The Smart Metering Information System validates the message.

3) The Smart Metering Information System applies new or updated settings.

4) The Smart Metering Information System sends a communication to the Asset Entity confirming the application of the settings.

Maintain Basic Flow:

1) The Smart Metering Information System identifies that a part of its system has either reached the end of its natural life or is malfunctioning and requires maintenance or the Asset Entity wishes to update the Smart Metering Information System software.

2) The Smart Metering Information System alerts the Asset Entity to the maintenance requirement(s) or the Asset Entity informs the Smart Metering Information System that a software update is to be performed.

3) The Asset Entity receives the alert and assesses whether the maintenance requirement necessitates a software or hardware update or requires an on-site visit.

4) The Asset Entity takes appropriate action to maintain the Smart Metering Information System.

5) The Smart Metering Information System receives the update from the Asset Entity and applies it sending a message back to the Asset Entity.

6) The Smart Metering Information System re-runs the original diagnostic that identified the requirement for maintenance. If the maintenance requirement is resolved nothing happens. If the maintenance requirement has not been resolved then go back to Step 2.

Alternative Flow:

1) The Smart Metering Information System does not recognise the request and deems it invalid.

2) The Smart Metering Information System does not apply the configuration settings.

3) The Smart Metering Information System sends a communication to the Asset Entity containing date/time stamp along with error details.

4) The Asset Entity is aware that a failure has occurred.

5) If a hardware update is required then the Asset Entity will arrange to visit the site of the Smart Metering Information System to install the required hardware.

6) The Asset Entity will send a message (or via another means e.g. verbal or postal notification directly to the Consumer) to the Smart Metering Information System detailing the appointment date and time (this is also applicable if the Asset Entity does not gain entry to the premise and an appointment re-schedule is needed).

7) The Smart Metering Information System will display the appointment date and time to the Consumer until the Consumer deletes or clears the message (if the message was notified via another means as noted above, the Consumer confirms acceptance or decline to the Asset Entity via an agreed process).

8) The Asset Entity visits the site of the Smart Metering Information System and replaces the required hardware. The Asset Entity updates the hardware details stored within the Smart Metering Information System.

9) The Smart Metering Information System will send a message to the Asset Entity informing them of the new hardware details.

5.2.4.5 Potential new requirements

- Network related functionality and managed M2M Devices or M2M Gateways should be monitored proactively in order to attempt to prevent and correct errors.
- Lifecycle management should apply to individual COs and to M2M Services.
- Static information such M2M capabilities may be assigned to M2M Devices and Gateways.
- The M2M System should support auto-configuration functions for M2M Area Networks.
- The M2M System should support accurate and secure time synchronisation. M2M Devices and M2M Gateways may support time synchronization or secure time synchronisation.
- The following management capabilities should be supported from the network side (i.e. manageability will depend on the end-system):
  - Secure software and firmware provisioning.
  - Configuration management.
  - Subscription management for M2M application provider:
    - Flexibility to choose M2M application provider after manufacture and after deployment of equipment.
    - Flexibility to change M2M application provider for already-deployed equipment (possibly without visiting the equipment).
- The M2M System should support the capability to remotely change the state of a M2M Device e.g. enable or disable.

- The M2M System should support mechanisms to perform simple and scalable provisioning of M2M Devices. The provisioning mechanism should be able to work when the communication path to the M2M Device is temporary absent.
  The M2M Application or Capabilities in the Service Capabilities should support autoconfiguration, that is without human intervention, of M2M Device or M2M Gateway when these are turned-on. The M2M Device or M2M Gateway may support autoconfiguration and registration to M2M Application functions.

- The M2M System should be able to authenticate the M2M Device or M2M Gateway. For M2M Devices supporting authentication and connected via an M2M Gateway, the authentication may be performed directly to the M2M System or to the authenticated M2M Gateway.

- When there is a request for data or device access, the M2M Device or M2M Gateway should be able to authenticate the M2M Service Capabilities or M2M Applications from which request is received.

- The M2M System should support a security solution that makes it impossible to acquire information about the data collected by eavesdropping at any point in the network. A particular application may or may not require the use of such security solution. Security solution should not prevent regulatory requirements such as lawful interception.

- End points of the M2M System should be able to verify the integrity of the data exchanged.

- Meter/Gateway swap out - the ability change a meter or gateway device and re-establish the HAN afterwards with minimal disruption.

5.2.4.6 Use case source

ESMIG, Document: Smart Metering Functionality Use Cases, ESMCR003-002-1.0, October 2009 [i.4].

5.2.5 Support Prepayment Functionality

5.2.5.1 General Use Case Description

This High Level Use Case is aligned to the "Additional Functionality" F3 described in clause 4.1.
It describes how the Smart Metering Information System is configured to support the Prepayment functionality as defined by the Bill Entity. The Use Case describes occasions where the Prepayment functionality is managed locally on the Smart Metering Information System as well as instances where the management occurs remotely by the Bill Entity.

5.2.5.2 Stakeholders

Bill Entity, Consumer, Asset Entity.

5.2.5.3 Scenario

Pre Conditions:

The Smart Metering Information System is installed and configured to act as a Prepayment meter.
The Smart Metering Information System recognises the Bill Entity and/or Asset Entity and has an address for them.

Post Conditions:

The Smart Metering Information System confirms to the Bill Entity and/or Asset Entity that a Prepayment action has been completed.
The Bill Entity and/or Asset Entity is made aware when a failure has occurred.

Trigger:

The Bill Entity or the consumer decides that there is a need to carry out a Prepayment action on the Smart Metering Information System.

5.2.5.4 Information Exchanges

Basic Flow:

1) The Asset Entity or Bill Entity sends a message to the Smart Metering Information System to change the payment mode.
2) The Smart Metering Information System validates the request.
3) The Smart Metering Information System changes the payment mode.
4) The Asset Entity or Bill Entity receives confirmation of the completion of payment mode change.
5) The Smart Metering Information System displays pre-configured information from the Asset Entity and/or Bill Entity.
6) The Consumer reads this information via a display.
7) The Consumer is able to act upon this information.
8) The Consumer undertakes an action as a result of this information e.g. adds credit to the Smart Metering Information System or releases the Emergency Credit facility.
9) The Smart Metering Information System sends confirmation messages back to the Asset Entity and/or Bill Entity when actions are completed.
10) The Smart Metering Information System provides status information at predetermined intervals or upon request from the Bill Entity.

Alternative Flow 1:

Fails at Step 2, Smart Metering Information System fails to validate request:

1) The Asset Entity or Bill Entity sends a message to the Smart Metering Information System to change the payment mode.
2) The Smart Metering Information System deems the request invalid, is unable to change payment mode or display the pre-configured information.
3) The Smart Metering Information System records the event (Error) along with date/time stamp.
4) The Smart Metering Information System notifies the Asset Entity and/or Bill Entity that a failure has occurred.
5) END.

Alternative Flow 2:

Fails at Step 3, Smart Metering Information System fails to change payment mode as requested:

1) The Asset Entity or Bill Entity sends a message to the Smart Metering Information System to change the payment mode.
2) The Smart Metering Information System validates the request.
3) The Smart Metering Information System fails to change the payment mode and deems the request invalid, is unable to change payment mode or display the pre-configured information.
4) The Smart Metering Information System records the event (Error) along with date/time stamp.
5) The Smart Metering Information System notifies the Asset Entity and/or Bill Entity that a failure has occurred.
6) END.

Alternative Flow 3:

Fails at Step 5, Smart Metering Information System fails to display pre-configured information from Asset Entity and/or Bill Entity:

1) The Asset Entity or Bill Entity sends a message to the Smart Metering Information System to change the payment mode.
2) The Smart Metering Information System validates the request.
3) The Smart Metering Information System changes the payment mode.
4) The Asset Entity or Bill Entity receives confirmation of the completion of payment mode change.
5) The Smart Metering Information System fails to display pre-configured information from the Asset Entity and/or Bill Entity.
6) The Smart Metering Information System deems the request invalid, is unable to display the pre-configured information.
7) The Smart Metering Information System records the event (Error) along with date/time stamp.
8) The Smart Metering Information System notifies the Asset Entity and/or Bill Entity that a failure has occurred.
9) END.

Alternative Flow 4:

Fails at Step 6, Consumer Fails to read information via display:

1) The Asset Entity or Bill Entity sends a message to the Smart Metering Information System to change the payment mode.
2) The Smart Metering Information System validates the request.
3) The Smart Metering Information System changes the payment mode.
4) The Asset Entity or Bill Entity receives confirmation of the completion of payment mode change.
5) The Smart Metering Information System displays pre-configured information from the Asset Entity and/or Bill Entity.
6) The Consumer fails to read this information via the display (Error).
7) After a specific period of time - The Smart Metering Information System deems the request invalid since customer has failed to read message and not acted upon information within message.
   [This assumes that customer has to accept this change].
8) The Smart Metering Information System records the event (Error) along with date/time stamp.
9) The Smart Metering Information System notifies the Asset Entity and/or Bill Entity that a failure has occurred.
10) END.

Alternative Flow 5:

Fails at Step 7, Consumer fails to act upon information shown via the display:

1) The Asset Entity or Bill Entity sends a message to the Smart Metering Information System to change the payment mode.
2) The Smart Metering Information System validates the request.
3) The Smart Metering Information System changes the payment mode.
4) The Asset Entity or Bill Entity receives confirmation of the completion of payment mode change.

5) The Smart Metering Information System displays pre-configured information from the Asset Entity and/or Bill Entity.

6) The Consumer reads this information via a display.

7) The Consumer is unable to act upon this information (Error).

8) The Smart Metering Information System deems that the customer is unable to change payment mode or display the pre-configured information
[This assumes that customer has to accept and act on change].

9) The Smart Metering Information System records the event (Error) along with date/time stamp.

10) The Smart Metering Information System notifies the Asset Entity and/or Bill Entity that a failure has occurred.

11) END.

Alternative Flow 6:

Fails at Step 9, Smart Metering Information System fails to send a confirmation message back to the Asset Entity and/or Bill Entity when actions are completed:

1) The Asset Entity or Bill Entity sends a message to the Smart Metering Information System to change the payment mode.

2) The Smart Metering Information System validates the request.

3) The Smart Metering Information System changes the payment mode.

4) The Asset Entity or Bill Entity receives confirmation of the completion of payment mode change.

5) The Smart Metering Information System displays pre-configured information from the Asset Entity and/or Bill Entity.

6) The Consumer reads this information via a display.

7) The Consumer is able to act upon this information.

8) The Consumer undertakes an action as a result of this information e.g. adds credit to the Smart Metering Information System or releases the Emergency Credit facility.

9) The Smart Metering Information System fails to send a confirmation messages back to the Asset Entity and/or Bill Entity when actions are completed.

10) The Smart Metering Information System deems that the customer is unable to change payment mode or display the pre-configured information
[This assumes that customer has to accept and act on change].

11) The Smart Metering Information System records the event (Error) along with date/time stamp.

12) The Smart Metering Information System notifies the Asset Entity and/or Bill Entity that a failure has occurred.

13) END.

5.2.5.5 Potential new requirements

- Use of the prepay switch/valve to enable control of the supply but not necessarily run the prepay application. In this instance, the metering system needs the ability to make known the fact that it is fitted with a switch/valve. The supply can then be interrupted and restored remotely.
- Static information such M2M capabilities may be assigned to M2M Devices and Gateways.
- The M2M System should support auto-configuration functions for M2M Area Networks.
- The M2M System should support accurate and secure time synchronisation. M2M Devices and M2M Gateways may support time synchronization or secure time synchronisation.

- The following management capabilities should be supported from the network side (i.e. manageability will depend on the end-system):
  - Secure software and firmware provisioning.
  - Configuration management.
  - Subscription management for M2M application provider:
    - Flexibility to choose M2M application provider after manufacture and after deployment of equipment.
    - Flexibility to change M2M application provider for already-deployed equipment (possibly without visiting the equipment).
- The M2M System should support the generation of charging information about the used M2M resources.
- The M2M System should support the mechanisms required for secured and traceable compensation and micro-compensation.
- M2M Application should be able to specify a periodic reporting of specific parameters for a specific M2M Device or group of M2M Devices. The M2M Application should be able to modify the value of the requested time period.
  In addition to the periodic reporting mechanism, M2M Application should be able to request the same report to the same M2M Device or group of M2M Devices in an on-demand mode.
- The M2M System should support the capability to remotely change the state of a M2M Device e.g. enable or disable.
- The M2M System should support transaction handling between cooperating objects capable of handling this functionality.
- The M2M System should support the following mechanisms for receiving information from M2M Devices and M2M Gateways:
  - Receiving unsolicited information (passive retrieval).
  - Receiving scheduled information.
- Operating particular algorithms for retrieving information (e.g., round robin, random within given time window, round robin groups with random reply in given time window).
- The M2M System should be able to authenticate the M2M Device or M2M Gateway. For M2M Devices supporting authentication and connected via an M2M Gateway, the authentication may be performed directly to the M2M System or to the authenticated M2M Gateway.
- The M2M System should support a security solution that makes it impossible to acquire information about the data collected by eavesdropping at any point in the network. A particular application may or may not require the use of such security solution. Security solution should not prevent regulatory requirements such as lawful interception.
- End points of the M2M System should be able to verify the integrity of the data exchanged.
- The M2M System should support mutual authentication and authorization between the end-user and the application or capability in the M2M service layer.
- The M2M System should support a mechanism for device integrity validation. The M2M Device may or may not support integrity validation. If the M2M Device supports integrity validation and if the device validation fails, the device should not be allowed to perform device authentication.
  The mechanism for device integrity validation may be initiated upon query from the M2M System or may be autonomously started locally by the M2M Device at any time.
  The M2M System may remotely get the historical log of tamper detection in a M2M Device if supported by the device.

5.2.5.6 Use case source

ESMIG, Document: Smart Metering Functionality Use Cases, ESMCR003-002-1.0, October 2009 [i.4].

5.2.6 Monitor Power Quality Data

5.2.6.1 General Use Case Description

This High Level Use Case is aligned to the "Additional Functionality" F2 described in clause 4.1.
The complexity of the system to move electric energy from the point of production to the point of consumption combined with variations in weather, generation, demand and other factors provide many opportunities for the quality of the supply to be compromised. Electrical devices may malfunction, fail prematurely or not operate at all.
This Use Case describes how the Smart Metering Information System provides power quality data. The Distribution Network Operator, Asset Entity or Consumer is able to use this data to monitor the Supply performance and if necessary instigate actions to ensure correct performance levels.

5.2.6.2 Stakeholders

Distribution Network Operator, Consumer, Asset Entity.

5.2.6.3 Scenario

Pre Conditions:

The Smart Metering Information System is installed and configured.
The Smart Metering Information System recognises the Distribution Network Operator and/or Asset Entity and has an address for them.
The Distribution Network Operator is able to receive Metering information from all systems connected for a particular distribution system.

Post Conditions:

The Distribution Network Operator and/or Asset Entity have received the requested power quality information.
The Distribution Network Operator and/or Asset Entity are aware that a failure has occurred (power quality parameters measured are beyond acceptable tolerance levels).
The Consumer has received the requested power quality information.

Trigger:

The Distribution Network Operator and/or Asset Entity decide there is a need to obtain power quality information from the Smart Metering Information System.

5.2.6.4 Information Exchanges

Basic Flow:

1) The Distribution Network Operator or Asset Entity sends a request to the Smart Metering Information System to obtain power quality information.

2) The Smart Metering Information System validates the request.

3) The Smart Metering Information System retrieves all power quality information along with date/time stamp.

4) The Smart Metering Information System sends the information to the Distribution Network Operator and/or Asset Entity.

Alternative Flow:

At Basic Flow step 2:

1) The Smart Metering Information System deems the request invalid e.g. not authorised.

2) The Smart Metering Information System sends a communication to the Distribution Network Operator or Asset Entity containing date/time stamp along with error details.

At Basic Flow step 3:

1) The Smart Metering Information System fails to retrieve the power quality information.

2) The Smart Metering Information System sends a communication to the Distribution Network Operator or Asset Entity containing date/time stamp along with error details.

At Basic Flow step 4:

1) The Distribution Network Operator or Asset Entity fails to receive the power quality information from the Smart Metering Information System.

2) The Distribution Network Operator and/or Asset Entity is aware that a failure has occurred.

3) The Distribution Network Operator or Asset Entity undertake follow-up actions to address the issue.

5.2.6.5 Potential new requirements

- The M2M System should support accurate and secure time synchronisation. M2M Devices and M2M Gateways may support time synchronization or secure time synchronisation.

- M2M Application should be able to specify a periodic reporting of specific parameters for a specific M2M Device or group of M2M Devices. The M2M Application should be able to modify the value of the requested time period.
  In addition to the periodic reporting mechanism, M2M Application should be able to request the same report to the same M2M Device or group of M2M Devices in an on-demand mode.

- The M2M System should support transaction handling between cooperating objects capable of handling this functionality.

- The M2M System should support the following mechanisms for receiving information from M2M Devices and M2M Gateways:

  - Receiving unsolicited information (passive retrieval).

  - Receiving scheduled information.

  - Operating particular algorithms for retrieving information (e.g., round robin, random within given time window, round robin groups with random reply in given time window).

- The M2M System should be able to authenticate the M2M Device or M2M Gateway. For M2M Devices supporting authentication and connected via an M2M Gateway, the authentication may be performed directly to the M2M System or to the authenticated M2M Gateway.

- When there is a request for data or device access, the M2M Device or M2M Gateway should be able to authenticate the M2M Service Capabilities or M2M Applications from which request is received.

- The M2M System should support a security solution that makes it impossible to acquire information about the data collected by eavesdropping at any point in the network. A particular application may or may not require the use of such security solution. Security solution should not prevent regulatory requirements such as lawful interception.

- End points of the M2M System should be able to verify the integrity of the data exchanged.

- The M2M System should support mutual authentication and authorization between the end-user and the application or capability in the M2M service layer.

- M2M devices that require device integrity validation should provide a trusted execution environment. The Trusted Environment (TrE) should be a logical entity which provides a trustworthy environment for the execution of sensitive functions and the storage of sensitive data. All data produced through execution of functions within the TrE should be unknowable to unauthorized external entities. The TrE should perform sensitive functions (such as storing secret keys and providing cryptographic calculations using those secret keys) needed to perform M2M device integrity check and device validation.

5.2.6.6 Use case source

ESMIG, Document: Smart Metering Functionality Use Cases, ESMCR003-002-1.0, October 2009 [i.4].

5.2.7 Manage Outage Data

5.2.7.1 General Use Case Description

This High Level Use Case is aligned to the "Additional Functionality" F2 described in clause 4.1.
It describes how the Distribution Network Operator provides data to the Smart Metering Information System relating to a planned outage. In addition, the Smart Metering Information System may also provide information relating to unplanned outages to the Distribution Network Operator and/or Bill Entity.

5.2.7.2 Stakeholders

Distribution Network Operator, Bill Entity, Consumer.

5.2.7.3 Scenario

Pre Conditions:

The Smart Metering Information System is installed and configured to detect supply outages and send messages detailing the outages to the Distribution Network Operator.
The Smart Metering Information System recognises the Distribution Network Operator and/or Bill Entity and has an address for it.

Post Conditions:

The Distribution Network Operator receives the requested outage information.
The Distribution Network Operator is aware that a failure has occurred.

Trigger:

Supply is interrupted (unplanned outage) to the Smart Metering Information System.
The Distribution Network Operator decides that a planned outage is to be carried out.

5.2.7.4 Information Exchanges

Basic Flow (for unplanned outages):

1) The Distribution Network Operator sends a request to the Smart Metering Information System to obtain outage information.

2) The Smart Metering Information System validates the request.

3) The Smart Metering Information System retrieves all outage information along with date/time stamps.

4) The Smart Metering Information System sends the information to the Distribution Network Operator or Bill Entity.

5) The Distribution Network Operator or Bill Entity receives the information.

Alternative Flow 1 (for unplanned outages):

Fails at Step 2:

1) The Distribution Network Operator sends a request to the Smart Metering Information System to obtain outage information.

2) The Smart Metering Information System deems the request or message invalid.

3) The Smart Metering Information System sends a communication to the Distribution Network Operator containing date/time stamp along with error details.

4) The Consumer's display is updated with the event.

5) END.

Alternative Flow 2 (for unplanned outages):

Fails at Step 3, Smart Metering Information System fails to retrieve outage information:

1) The Distribution Network Operator sends a request to the Smart Metering Information System to obtain outage information.

2) The Smart Metering Information System validates the request.

3) Smart Metering Information System fails to retrieve outage information and/or date/time stamp information.

4) The Smart Metering Information System deems the request or message invalid.

5) The Smart Metering Information System sends a communication to the Distribution Network Operator containing date/time stamp along with error details.

6) The Consumer's display is updated with the event.

7) END.

Alternative Flow 3 (for unplanned outages):

Fails at Step 4, Smart Metering Information System fails to send information to Distribution Network Operator / Bill Entity:

1) The Distribution Network Operator sends a request to the Smart Metering Information System to obtain outage information.

2) The Smart Metering Information System validates the request.

3) The Smart Metering Information System retrieves all outage information along with date/time stamps.

4) The Smart Metering Information System fails to send the information to the Distribution Network Operator or Bill Entity.

5) The Smart Metering Information System deems the request or message invalid.

6) The Smart Metering Information System sends a communication to the Distribution Network Operator containing date/time stamp along with error details.

7) The Consumer's display is updated with the event.

8) END.

Alternative Flow 4 (for unplanned outages):

Fails at Step 5, Distribution Network Operator or Bill Entity fails to receive information from Smart Metering Information System:

1) The Distribution Network Operator sends a request to the Smart Metering Information System to obtain outage information.

2) The Smart Metering Information System validates the request.

3) The Smart Metering Information System retrieves all outage information along with date/time stamps.

4) The Smart Metering Information System sends the information to the Distribution Network Operator or Bill Entity.

5) Distribution Network Operator or Bill Entity fails to receive the information.

6) The Smart Metering Information System deems the request or message invalid.

7) The Smart Metering Information System sends a communication to the Distribution Network Operator containing date/time stamp along with error details.

8) The Consumer's display is updated with the event.

9) END.

Basic Flow (for planned outages):

1) The Distribution Network Operator sends information to the Smart Metering Information System detailing a planned outage.

2) The Smart Metering Information System validates the message.

3) The Smart Metering Information System displays the message to the Consumer.

4) The Consumer accepts the message.

5) The Smart Metering Information System sends confirmation back to the Distribution Network Operator that the planned outage message has been accepted.

Alternative Flow 1 (for planned outages):

Fails at Step 2:

1) The Distribution Network Operator sends information to the Smart Metering Information System detailing a planned outage.

2) The Smart Metering Information System deems the request or message invalid.

3) The Smart Metering Information System sends a communication to the Distribution Network Operator containing date/time stamp along with error details.

4) The Consumer's display is updated with the event.

5) END.

Alternative Flow 2 (for planned outages):

Fails at Step 3:

1) The Distribution Network Operator sends information to the Smart Metering Information System detailing a planned outage.

2) The Smart Metering Information System validates the message.

3) Smart Metering Information System fails to display message to the Consumer.

4) The Smart Metering Information System deems the request or message invalid.

5) The Smart Metering Information System sends a communication to the Distribution Network Operator containing date/time stamp along with error details.

6) The Consumer's display is updated with the event.

7) END.

Alternative Flow 3 (for planned outages):

Fails at Step 4:

1) The Distribution Network Operator sends information to the Smart Metering Information System detailing a planned outage.
2) The Smart Metering Information System validates the message.
3) The Smart Metering Information System displays the message to the Consumer.
4) The Consumer does not accept the message.
5) The Smart Metering Information System deems the request or message invalid.
6) The Smart Metering Information System sends a communication to the Distribution Network Operator containing date/time stamp along with error details.
7) The Consumer's display is updated with the event.
8) END.

Alternative Flow 4 (for planned outages):

Fails at Step 5:

1) The Distribution Network Operator sends information to the Smart Metering Information System detailing a planned outage.
2) The Smart Metering Information System validates the message.
3) The Smart Metering Information System displays the message to the Consumer.
4) The Consumer accepts the message.
5) The Smart Metering Information System fails to send confirmation back to the Distribution Network Operator that a planned outage message has been accepted.
6) The Smart Metering Information System deems the request or message invalid.
7) The Smart Metering Information System sends a communication to the Distribution Network Operator containing date/time stamp along with error details.
8) The Consumer's display is updated with the event.
9) END.

5.2.7.5 Potential new requirements

- The M2M System should support accurate and secure time synchronisation. M2M Devices and M2M Gateways may support time synchronization or secure time synchronisation.
- M2M Application should be able to specify a periodic reporting of specific parameters for a specific M2M Device or group of M2M Devices. The M2M Application should be able to modify the value of the requested time period.
  In addition to the periodic reporting mechanism, M2M Application should be able to request the same report to the same M2M Device or group of M2M Devices in an on-demand mode.
- The M2M System should support transaction handling between cooperating objects capable of handling this functionality.
- The M2M System should support the following mechanisms for receiving information from M2M Devices and M2M Gateways:
  - Receiving unsolicited information (passive retrieval).
  - Receiving scheduled information.

- Operating particular algorithms for retrieving information (e.g., round robin, random within given time window, round robin groups with random reply in given time window).

- An object may be able to communicate in a peer-to-peer manner with any other connected object. In this case, packet flows should be supported between these objects.

- The M2M System should be able to authenticate the M2M Device or M2M Gateway. For M2M Devices supporting authentication and connected via an M2M Gateway, the authentication may be performed directly to the M2M System or to the authenticated M2M Gateway.

- When there is a request for data or device access, the M2M Device or M2M Gateway should be able to authenticate the M2M Service Capabilities or M2M Applications from which request is received.

- The M2M System should support a security solution that makes it impossible to acquire information about the data collected by eavesdropping at any point in the network. A particular application may or may not require the use of such security solution. Security solution should not prevent regulatory requirements such as lawful interception.

- End points of the M2M System should be able to verify the integrity of the data exchanged.

- The M2M System should support mutual authentication and authorization between the end-user and the application or capability in the M2M service layer.

- M2M devices that require device integrity validation should provide a trusted execution environment. The Trusted Environment (TrE) should be a logical entity which provides a trustworthy environment for the execution of sensitive functions and the storage of sensitive data. All data produced through execution of functions within the TrE should be unknowable to unauthorized external entities. The TrE should perform sensitive functions (such as storing secret keys and providing cryptographic calculations using those secret keys) needed to perform M2M device integrity check and device validation.

5.2.7.6 Use case source

ESMIG, Document: Smart Metering Functionality Use Cases, ESMCR003-002-1.0, October 2009 [i.4].

5.2.8 Facilitate Demand Response Actions

5.2.8.1 General Use Case Description

This Use Case is aligned to the "Additional Functionality" F5 and F6 described in clause 4.1.
It describes how the Distribution Network Operator and/or the Efficiency Entity provide an instruction(s) relating to demand response to the Smart Metering Information System.
It also describes High Level how the Consumer uses a display unit to view details from the Network Operator and/or the Efficiency Entity prior to the Consumer instigating the demand response action.

5.2.8.2 Stakeholders

Distribution Network Operator, Consumer, Efficiency Entity, Bill Entity, Energy Services Provider.

5.2.8.3 Scenario

Pre Conditions:

The Smart Metering Information System is installed and configured to accept and display messages and send delivery receipts.

The Smart Metering Information System recognises the Distribution Network Operator and/or Efficiency Entity and/or Bill Entity, Energy Services Provider and has an address for them.

The Consumer has a contract with the Distribution Network Operator and/or Efficiency Entity and/or Bill Entity.
The Consumer understands how to reduce demand in response to an instruction message.

Post Conditions:

The Consumer approves or declines instruction from the Distribution Network Operator and/or Efficiency Entity and/or Bill Entity.
The change in demand required by the Distribution Network Operator and/or Efficiency Entity and/or Bill Entity has occurred.
The Distribution Network Operator and/or Efficiency Entity and/or Bill Entity are aware when a failure has occurred.

Trigger:

The Distribution Network Operator and/or Efficiency Entity and/or Bill Entity wishes to change the level of Consumer consumption via a demand response event.

5.2.8.4 Information Exchanges

Basic Flow:

1) The Distribution Network Operator or Efficiency Entity sends a message to the Smart Metering Information System notifying of a demand response event.

2) The Smart Metering Information System receives the message from the Distribution Network Operator or Efficiency Entity. (The message may be targeted at a particular device/appliance which may modify its settings or turn it off/on.)

3) The Smart Metering Information System validates the message.

4) The Smart Metering Information System displays a message indicating that a load control activity is about to be undertaken (including details of the action to be taken).

5) The Consumer reads the message via a display.

6) The Consumer accepts the message or may choose to override the command.

7) The Consumer deletes or saves the message.

8) The Smart Metering Information System sends a message to the Distribution Network Operator or Efficiency Entity or Bill Entity confirming the Consumer's action.

9) The Consumer undertakes an action as a result.

NOTE: This could be initiating a demand response or ignoring the pricing notification and doing nothing.

10) The Smart Metering Information System sends energy volume data to the Distribution Network Operator or Efficiency Entity or Bill Entity as per the agreed schedule.

11) The Distribution Network Operator or Efficiency Entity or Bill Entity checks that the Consumer has complied with the demand response event (some occasions the Consumer may be contractually obliged and the Distribution Network Operator and/or Bill Entity may levy fines if necessary).

Alternative Flow:

At Basic Flow step 3:

1) The Smart Metering Information System deems the message invalid.

2) The Smart Metering Information System sends a rejection message to the Distribution Network Operator or Efficiency Entity or Bill Entity along with date/time stamp and error type.

At Basic Flow steps 8:

1) The Smart Metering Information System fails to send information to the Distribution Network Operator and/or Efficiency Entity and/or Bill Entity.

2) The Distribution Network Operator and/or Efficiency Entity and/or Bill Entity is aware that a failure has occurred.

5.2.8.5 Potential new requirements

- The M2M System should support accurate and secure time synchronisation. M2M Devices and M2M Gateways may support time synchronization or secure time synchronisation.
- M2M Application should be able to specify a periodic reporting of specific parameters for a specific M2M Device or group of M2M Devices. The M2M Application should be able to modify the value of the requested time period.
  In addition to the periodic reporting mechanism, M2M Application should be able to request the same report to the same M2M Device or group of M2M Devices in an on-demand mode.
- The M2M System should support transaction handling between cooperating objects capable of handling this functionality.
- The M2M System should support the following mechanisms for receiving information from M2M Devices and M2M Gateways:
  - Receiving unsolicited information (passive retrieval).
  - Receiving scheduled information.
  - Operating particular algorithms for retrieving information (e.g., round robin, random within given time window, round robin groups with random reply in given time window).
- An object may be able to communicate in a peer-to-peer manner with any other connected object. In this case, packet flows should be supported between these objects.
- The M2M System should be able to authenticate the M2M Device or M2M Gateway. For M2M Devices supporting authentication and connected via an M2M Gateway, the authentication may be performed directly to the M2M System or to the authenticated M2M Gateway.
- When there is a request for data or device access, the M2M Device or M2M Gateway should be able to authenticate the M2M Service Capabilities or M2M Applications from which request is received.
- The M2M System should support a security solution that makes it impossible to acquire information about the data collected by eavesdropping at any point in the network. A particular application may or may not require the use of such security solution. Security solution should not prevent regulatory requirements such as lawful interception.
- End points of the M2M System should be able to verify the integrity of the data exchanged.
- The M2M System should support mutual authentication and authorization between the end-user and the application or capability in the M2M service layer.
- M2M devices that require device integrity validation should provide a trusted execution environment. The Trusted Environment (TrE) should be a logical entity which provides a trustworthy environment for the execution of sensitive functions and the storage of sensitive data. All data produced through execution of functions within the TrE should be unknowable to unauthorized external entities. The TrE should perform sensitive functions (such as storing secret keys and providing cryptographic calculations using those secret keys) needed to perform M2M device integrity check and device validation.

5.2.8.6 Use case source

ESMIG, Document: Smart Metering Functionality Use Cases, ESMCR003-002-1.0, October 2009 [i.4].

5.2.9 Facilitate Distributed Generation Actions

5.2.9.1 General Use Case Description

This High Level Use Case is aligned to the "Additional Functionality" F1 and F6 described in clause 4.1.
It describes how the Distribution Network Operator and/or Efficiency Entity and/or Bill Entity provide instruction relating to distributed generation to the Smart Metering Information System. This Use Case considers the specific situation for electricity where there may be distributed generating units such as solar units, wind turbines, microgenerators in the home etc. which pose specific problems for controlling the electricity distribution network.
This Use Case deals with the scenario where the Consumer's equipment could be programmed to generate at an up to predefined level. It also describes how the Consumer uses a display unit to view details from the Distribution Network Operator and/or the Efficiency Entity and/or Bill Entity prior to instigating the distributed generation action (e.g. to initiate or stop generation).

5.2.9.2 Stakeholders

Distribution Network Operator, Consumer, Efficiency Entity, Bill Entity.

5.2.9.3 Scenario

Pre Conditions:

The facility to generate electricity (distributed generation) is available at the premises.

The Smart Metering Information System is installed and configured to send information to and from the Distribution Network Operator and/or Bill Entity.
The Consumer may have a contract with the Distribution Network Operator and/or Bill Entity to receive credit for generation or export (or both).
The Smart Metering Information System recognises the Distribution Network Operator and/or the Efficiency Entity and/or Bill Entity and has an address for it.
The Distribution Network Operator and/or Bill Entity is able to receive Metering information from all systems connected for a particular distribution system.
The Distribution Network Operator and/or Bill Entity is able to receive information from generators and meteorological information (e.g. wind and sun).

Post Conditions:

The Smart Metering Information System has provided net energy, generated energy and consumed energy values to the Distribution Network Operator and/or Efficiency Entity and/or Bill Entity.
The Distribution Network Operator and/or the Efficiency Entity and/or Bill Entity is aware that a failure has occurred.

Trigger:

The Distribution Network Operator has a requirement to balance renewable and non-renewable generation with demand.
The Consumer and/or the Efficiency Entity decides that there is a need to generate power at the Consumer's premise or the Consumer's equipment is programmed to generate continuously at a predefined generation level.

5.2.9.4 Information Exchanges

Basic Flow:

1) The Distribution Network Operator identifies unfavourable market conditions (e.g. loss of generation, loss of transmission lines or overloaded transformers), the Consumer and/or the Efficiency Entity decides to instigate a distributed generation event or the Consumer's equipment is programmed to generate continuously.

2) The Distribution Network Operator determines what generation can be brought on line to resolve the issue, the Consumer and/or the Efficiency Entity decides on the level of generation or the Consumer's equipment generates at a predefined level.

3) If the trigger is the Distribution Network Operator, it sends a request to the Smart Metering Information System to:

   - increase / decrease demand;
   - increase / decrease generation.

4) The Smart Metering Information System validates the request.

5) The Consumer's equipment acknowledges the request.

6) The Smart Metering Information System records the bi-directional flow of energy logging the generation from the Consumer side of the meter as well as the energy from the distribution side - this applies to various conditions triggering the distributed generation event.

7) The Smart Metering Information System displays amount of electricity generated versus that consumed on a display (if present) or on the Smart Metering Information System display when accessed by the Consumer.

8) The Smart Metering Information System records the quality of the electricity generated at the premise.

9) The Smart Metering Information System sends the net energy, generation, consumption and power quality information to the Distribution Network Operator and/or the Efficiency Entity and/or Bill Entity according to the agreed timetable.

10) The Distribution Network Operator and/or the Efficiency Entity and/or Bill Entity receives the energy information from the Smart Metering Information System and credits generated energy or net consumption to the Consumer's account.

Alternative Flow:

At Basic Flow step 4:

1) The Smart Metering Information System deems the request invalid.

2) The Smart Metering Information System sends a message to the Distribution Network Operator and/or the Efficiency Entity and/or Bill Entity detailing error type along with date/time stamp.

3) The Distribution Network Operator and/or the Efficiency Entity and/or Bill Entity undertakes a subsequent action to address the error.

At Basic Flow step 10:

1) The Distribution Network Operator and/or the Efficiency Entity and/or Bill Entity fails to receive the information from the Smart Metering Information System.

2) The Distribution Network Operator and/or the Efficiency Entity and/or Bill Entity is aware that an error has occurred.

5.2.9.5 Potential new requirements

- The M2M System should support accurate and secure time synchronisation. M2M Devices and M2M Gateways may support time synchronization or secure time synchronisation.
- M2M Application should be able to specify a periodic reporting of specific parameters for a specific M2M Device or group of M2M Devices. The M2M Application should be able to modify the value of the requested time period.
  In addition to the periodic reporting mechanism, M2M Application should be able to request the same report to the same M2M Device or group of M2M Devices in an on-demand mode.
- The M2M System should support the capability to remotely change the state of a M2M Device e.g. enable or disable.
- The M2M System should support transaction handling between cooperating objects capable of handling this functionality.

- The M2M System should support the following mechanisms for receiving information from M2M Devices and M2M Gateways:
  - Receiving unsolicited information (passive retrieval).
  - Receiving scheduled information.
  - Operating particular algorithms for retrieving information (e.g., round robin, random within given time window, round robin groups with random reply in given time window).
- An object may be able to communicate in a peer-to-peer manner with any other connected object. In this case, packet flows should be supported between these objects.
- The M2M System should be able to authenticate the M2M Device or M2M Gateway. For M2M Devices supporting authentication and connected via an M2M Gateway, the authentication may be performed directly to the M2M System or to the authenticated M2M Gateway.
- When there is a request for data or device access, the M2M Device or M2M Gateway should be able to authenticate the M2M Service Capabilities or M2M Applications from which request is received.
- The M2M System should support a security solution that makes it impossible to acquire information about the data collected by eavesdropping at any point in the network. A particular application may or may not require the use of such security solution. Security solution should not prevent regulatory requirements such as lawful interception.
- End points of the M2M System should be able to verify the integrity of the data exchanged.
- The M2M System should support mutual authentication and authorization between the end-user and the application or capability in the M2M service layer.
- M2M devices that require device integrity validation should provide a trusted execution environment. The Trusted Environment (TrE) should be a logical entity which provides a trustworthy environment for the execution of sensitive functions and the storage of sensitive data. All data produced through execution of functions within the TrE should be unknowable to unauthorized external entities. The TrE should perform sensitive functions (such as storing secret keys and providing cryptographic calculations using those secret keys) needed to perform M2M device integrity check and device validation.

5.2.9.6 Use case source

ESMIG, Document: Smart Metering Functionality Use Cases, ESMCR003-002-1.0, October 2009 [i.4].

5.2.10 Manage the Distribution Network using Smart Metering Information System Data

5.2.10.1 General Use Case Description

This High Level Use Case is aligned to the "Additional Functionality" F1 described in clause 4.1.
It describes how the Distribution Network Operator uses data from the Smart Metering Information System and/or from defined points across the Distribution Network to optimise current asset utilisation and/or optimise future asset planning.
This facilitates better management of the Distribution Network Operator's Distribution Network through informed decision making based on accurate and timely data from the Smart Metering Information System(s).

5.2.10.2 Stakeholders

Distribution Network Operator.

5.2.10.3 Scenario

Pre Conditions:

The Smart Metering Information System is installed and configured.
The Smart Metering Information System recognises the Distribution Network Operator and has an address for it.
The Smart Metering Information System collects and is able to provide data including readings and power quality measurements.

Post Conditions:

The Distribution Network Operator carries out a subsequent action to optimise planning or utilisation of assets following provision of information from the Smart Metering Information System.
The Distribution Network Operator is aware that a failure has occurred.

Trigger:

The Distribution Network Operator decides to utilise Smart Metering Information System data to optimise planning or utilisation of assets in its Distribution Network.

5.2.10.4 Information Exchanges

Basic Flow:

1) The Distribution Network Operator requests data from the Smart Metering Information System.
2) The Smart Metering Information System validates the request.
3) The Smart Metering Information System sends the requested data to the Distribution Network Operator.
4) The Distribution Network Operator validates data received from the Smart Metering Information System.
5) The Distribution Network Operator carries out a subsequent action to optimise planning or utilisation of assets.

Alternative Flow:

At Basic Flow step 2:

1) The Smart Metering Information System deems the request invalid.
2) The Smart Metering Information System sends notification to the Distribution Network Operator detailing error type along with date/time stamp.

At Basic Flow step 4:

1) The Distribution Network Operator fails to receive the requested information from the Smart Metering Information System or deems the data received from the Smart Metering Information System as invalid.
2) The Distribution Network Operator is aware that a failure has occurred.

5.2.10.5 Potential new requirements

- The M2M System should support accurate and secure time synchronisation. M2M Devices and M2M Gateways may support time synchronization or secure time synchronisation.
- M2M Application should be able to specify a periodic reporting of specific parameters for a specific M2M Device or group of M2M Devices. The M2M Application should be able to modify the value of the requested time period.
  In addition to the periodic reporting mechanism, M2M Application should be able to request the same report to the same M2M Device or group of M2M Devices in an on-demand mode.
- The M2M System should support the capability to remotely change the state of a M2M Device e.g. enable or disable.

- The M2M System should support transaction handling between cooperating objects capable of handling this functionality.
- The M2M System should support the following mechanisms for receiving information from M2M Devices and M2M Gateways:
  - Receiving unsolicited information (passive retrieval).
  - Receiving scheduled information.
  - Operating particular algorithms for retrieving information (e.g., round robin, random within given time window, round robin groups with random reply in given time window).
- An object may be able to communicate in a peer-to-peer manner with any other connected object. In this case, packet flows should be supported between these objects.
- The M2M System should be able to authenticate the M2M Device or M2M Gateway. For M2M Devices supporting authentication and connected via an M2M Gateway, the authentication may be performed directly to the M2M System or to the authenticated M2M Gateway.
- When there is a request for data or device access, the M2M Device or M2M Gateway should be able to authenticate the M2M Service Capabilities or M2M Applications from which request is received.
- The M2M System should support a security solution that makes it impossible to acquire information about the data collected by eavesdropping at any point in the network. A particular application may or may not require the use of such security solution. Security solution should not prevent regulatory requirements such as lawful interception.
- End points of the M2M System should be able to verify the integrity of the data exchanged.
- The M2M System should support mutual authentication and authorization between the end-user and the application or capability in the M2M service layer.
- M2M devices that require device integrity validation should provide a trusted execution environment. The Trusted Environment (TrE) should be a logical entity which provides a trustworthy environment for the execution of sensitive functions and the storage of sensitive data. All data produced through execution of functions within the TrE should be unknowable to unauthorized external entities. The TrE should perform sensitive functions (such as storing secret keys and providing cryptographic calculations using those secret keys) needed to perform M2M device integrity check and device validation.

5.2.10.6 Use case source

ESMIG, Document: Smart Metering Functionality Use Cases, ESMCR003-002-1.0, October 2009 [i.4].

5.2.11 Manage Interference and Malfunctions to the Smart Metering Information System

5.2.11.1 General Use Case Description

This High Level Use Case is aligned to the "Additional Functionality" F2 described in clause 4.1.
It describes how the Smart Metering Information System provides details of interference and malfunctions to its functionalities to the Asset Entity. Interference and malfunctions are threats that may compromise the confidentiality, integrity and availability of the Smart Metering Information System.

Interference is deemed to be unauthorised and can be deliberate (or illicit) or accidental (or innocent) - its management is in the form of event detection and prevention. Event detection and prevention is also applicable to the management of malfunctions on the Smart Metering Information System.

The Asset Entity receives this data and manages follow-up actions to address the interference and/or malfunctions. This may including making changes to Smart Metering Information System configuration on site or remotely, or replacing the entire Smart Metering Information System.

5.2.11.2 Stakeholders

Asset Entity, Bill Entity, Interference Entity.

5.2.11.3 Scenario

Pre Conditions:

The Smart Metering Information System is installed and configured.
The Smart Metering Information System recognises the Asset Entity and has an address or addresses for it.
The interference and/or malfunctions event logs and history are available for provision to the Asset Entity.

Post Conditions:

The Asset Entity undertakes subsequent actions as per defined internal processes following receipt of interference and/or malfunction information.
The Asset Entity is aware that an error has occurred.

Trigger:

An interference and/or malfunction event occurs which is detected by the Smart Metering Information System as per its defined settings/parameters.

5.2.11.4 Information Exchanges

Basic Flow:

1) The Smart Metering Information System sends a notification to the Asset Entity that an interference and/or malfunction event has been detected on the Smart Metering Information System.

2) The Asset Entity requests details of event and/or events history from the Smart Metering Information System.

3) The Smart Metering Information System validates the request.

4) The Smart Metering Information System sends the information to the Asset Entity.

5) The Asset Entity undertakes a subsequent action to address the issue.

Alternative Flow:

At Basic Flow step 3:

1) The Smart Metering Information System deems the request invalid.

2) The Smart Metering Information System sends notification to the Asset Entity detailing the error type along with date/time stamp.

At Basic Flow step 4:

1) The Asset Entity fails to receive the requested information from the Smart Metering Information System.

2) The Asset Entity is aware that a failure has occurred.

5.2.11.5 Potential new requirements

- The M2M System should support accurate and secure time synchronisation. M2M Devices and M2M Gateways may support time synchronization or secure time synchronisation.

- M2M Application should be able to specify a periodic reporting of specific parameters for a specific M2M Device or group of M2M Devices. The M2M Application should be able to modify the value of the requested time period.
  In addition to the periodic reporting mechanism, M2M Application should be able to request the same report to the same M2M Device or group of M2M Devices in an on-demand mode.

- The M2M System should support the capability to remotely change the state of a M2M Device e.g. enable or disable.
- The M2M System should support transaction handling between cooperating objects capable of handling this functionality.
- The M2M System should support the following mechanisms for receiving information from M2M Devices and M2M Gateways:
  - Receiving unsolicited information (passive retrieval).
  - Receiving scheduled information.
  - Operating particular algorithms for retrieving information (e.g., round robin, random within given time window, round robin groups with random reply in given time window).
- An object may be able to communicate in a peer-to-peer manner with any other connected object. In this case, packet flows should be supported between these objects.
- The M2M System should be able to authenticate the M2M Device or M2M Gateway. For M2M Devices supporting authentication and connected via an M2M Gateway, the authentication may be performed directly to the M2M System or to the authenticated M2M Gateway.
- When there is a request for data or device access, the M2M Device or M2M Gateway should be able to authenticate the M2M Service Capabilities or M2M Applications from which request is received.
- The M2M System should support a security solution that makes it impossible to acquire information about the data collected by eavesdropping at any point in the network. A particular application may or may not require the use of such security solution. Security solution should not prevent regulatory requirements such as lawful interception.
- End points of the M2M System should be able to verify the integrity of the data exchanged.
- The M2M System should support mutual authentication and authorization between the end-user and the application or capability in the M2M service layer.
- M2M devices that require device integrity validation should provide a trusted execution environment. The Trusted Environment (TrE) should be a logical entity which provides a trustworthy environment for the execution of sensitive functions and the storage of sensitive data. All data produced through execution of functions within the TrE should be unknowable to unauthorized external entities. The TrE should perform sensitive functions (such as storing secret keys and providing cryptographic calculations using those secret keys) needed to perform M2M device integrity check and device validation.

5.2.11.6 Use case source

ESMIG, Document: Smart Metering Functionality Use Cases, ESMCR003-002-1.0, October 2009 [i.4].

5.2.12 Manage Tariff Settings on the Smart Metering Information System

5.2.12.1 General Use Case Description

This High Level Use Case is aligned to the "Additional Functionality" F3 described in clause 4.1.
It describes how the Smart Metering Information System provides tariff and price information to the Consumer as per a predefined schedule or as a result of ad-hoc notifications from the Bill Entity.
Examples of this Use Case may include amending unit price on the Smart Metering Information System following a change in tariff and where the Smart Metering Information System is switched between 1 or 2 rate metering.

5.2.12.2 Stakeholders

Bill Entity, Consumer.

5.2.12.3 Scenario

Pre Conditions:

The Smart Metering Information System is installed and configured.
The Smart Metering Information System recognises the Bill Entity and has an address for them.

Post Conditions:

The Consumer is aware of new/updated tariffs formulated by the Bill Entity.
The Bill Entity is aware when a failure has occurred.

Trigger:

A defined point in the provision schedule is reached or the Bill Entity decides to send an ad-hoc notification to the Smart Metering Information System.

5.2.12.4 Information Exchanges

Basic Flow:

1) The Bill Entity sends an instruction to the Smart Metering Information System to apply new/updated tariff and price settings.

2) The Smart Metering Information System validates the request.

3) The Smart Metering Information System applies new/updated tariff and price settings.

4) The Consumer's display is updated with the information.

5) The Consumer saves or deletes the message.

6) The Smart Metering Information System sends a message to the Bill Entity confirming that the action has been carried out and that the Consumer has viewed the message.

Alternative Flow:

At Basic Flow step 2:

1) The Smart Metering Information System deems the request invalid.

2) The Smart Metering Information System sends notification to the Bill Entity detailing error type along with date/time stamp.

At Basic Flow step 6:

1) The Bill Entity does not receive confirmation from the Smart Metering Information System that the action has been carried out and/or the Consumer has not viewed the message.

2) The Bill Entity is aware that a failure has occurred.

5.2.12.5 Potential new requirements

- The M2M System should support accurate and secure time synchronisation. M2M Devices and M2M Gateways may support time synchronization or secure time synchronisation.

- M2M Application should be able to specify a periodic reporting of specific parameters for a specific M2M Device or group of M2M Devices. The M2M Application should be able to modify the value of the requested time period.
  In addition to the periodic reporting mechanism, M2M Application should be able to request the same report to the same M2M Device or group of M2M Devices in an on-demand mode.

- The M2M System should support the capability to remotely change the state of a M2M Device e.g. enable or disable.

- The M2M System should support transaction handling between cooperating objects capable of handling this functionality.
- The M2M System should support the following mechanisms for receiving information from M2M Devices and M2M Gateways:
  - Receiving unsolicited information (passive retrieval).
  - Receiving scheduled information.
  - Operating particular algorithms for retrieving information (e.g., round robin, random within given time window, round robin groups with random reply in given time window).
- An object may be able to communicate in a peer-to-peer manner with any other connected object. In this case, packet flows should be supported between these objects.
- The M2M System should be able to authenticate the M2M Device or M2M Gateway. For M2M Devices supporting authentication and connected via an M2M Gateway, the authentication may be performed directly to the M2M System or to the authenticated M2M Gateway.
- When there is a request for data or device access, the M2M Device or M2M Gateway should be able to authenticate the M2M Service Capabilities or M2M Applications from which request is received.
- The M2M System should support a security solution that makes it impossible to acquire information about the data collected by eavesdropping at any point in the network. A particular application may or may not require the use of such security solution. Security solution should not prevent regulatory requirements such as lawful interception.
- End points of the M2M System should be able to verify the integrity of the data exchanged.
- The M2M System should support mutual authentication and authorization between the end-user and the application or capability in the M2M service layer.
- M2M devices that require device integrity validation should provide a trusted execution environment. The Trusted Environment (TrE) should be a logical entity which provides a trustworthy environment for the execution of sensitive functions and the storage of sensitive data. All data produced through execution of functions within the TrE should be unknowable to unauthorized external entities. The TrE should perform sensitive functions (such as storing secret keys and providing cryptographic calculations using those secret keys) needed to perform M2M device integrity check and device validation.

5.2.12.6 Use case source

ESMIG, Document: Smart Metering Functionality Use Cases, ESMCR003-002-1.0, October 2009 [i.4].

5.2.13 Enable & Disable the Smart Metering Information System

5.2.13.1 General Use Case Description

This High Level Use Case is aligned to the "Additional Functionality" F4 described in clause 4.1.
It describes how the Asset Entity and/or the Bill Entity enable or disable the Smart Metering Information System according to predefined processes. This Use Case includes communication between the Asset Entity and/or the Bill Entity and the Smart Metering Information System and making changes to the Smart Metering Information System on site or remotely.
It also includes the application of actions to limit the product availability through the Smart Metering Information System.

5.2.13.2 Stakeholders

Asset Entity, Bill Entity.

5.2.13.3 Scenario

Pre Conditions:

The Smart Metering Information System is installed and configured.
The Smart Metering Information System recognises the Asset Entity and/or the Bill Entity and has an address for it.

Post Conditions:

The Asset Entity and/or the Bill Entity receives appropriate notification that supply has been enabled or disabled or product availability has been limited.
The Asset Entity and/or the Bill Entity is aware when a failure has occurred.

Trigger:

The Asset Entity and/or the Bill Entity decides to apply an action to enable or disable the supply or limit the product availability at the premise.

5.2.13.4 Information Exchanges

Basic Flow:

1) The Asset Entity and/or the Bill Entity send an instruction to the Smart Metering Information System to apply an action to enable or disable the supply or limit the product availability at the premise.

2) The Smart Metering Information System validates the request.

3) The Smart Metering Information System carries out the action.

4) The supply has been enabled or disabled or the product availability has been limited.

5) The Smart Metering Information System sends a message to the Asset Entity and/or the Bill Entity confirming that the action has been carried out.

Alternative Flow:

At Basic Flow step 2:

1) The Smart Metering Information System deems the request invalid.

2) The Smart Metering Information System sends notification to the Asset Entity and/or the Bill Entity detailing error type along with date/time stamp.

At Basic Flow step 5:

1) The Asset Entity and/or the Bill Entity does not receive confirmation from the Smart Metering Information System that the action has been carried out.

2) The Asset Entity and/or the Bill Entity is aware that a failure has occurred.

5.2.13.5 Potential new requirements

- The M2M System should support accurate and secure time synchronisation. M2M Devices and M2M Gateways may support time synchronization or secure time synchronisation.

- M2M Application should be able to specify a periodic reporting of specific parameters for a specific M2M Device or group of M2M Devices. The M2M Application should be able to modify the value of the requested time period.
  In addition to the periodic reporting mechanism, M2M Application should be able to request the same report to the same M2M Device or group of M2M Devices in an on-demand mode.

- The M2M System should support the capability to remotely change the state of a M2M Device e.g. enable or disable.

- The M2M System should support transaction handling between cooperating objects capable of handling this functionality.
- The M2M System should support the following mechanisms for receiving information from M2M Devices and M2M Gateways:
  - Receiving unsolicited information (passive retrieval).
  - Receiving scheduled information.
  - Operating particular algorithms for retrieving information (e.g., round robin, random within given time window, round robin groups with random reply in given time window).
- An object may be able to communicate in a peer-to-peer manner with any other connected object. In this case, packet flows should be supported between these objects.
- The M2M System should be able to authenticate the M2M Device or M2M Gateway. For M2M Devices supporting authentication and connected via an M2M Gateway, the authentication may be performed directly to the M2M System or to the authenticated M2M Gateway.
- When there is a request for data or device access, the M2M Device or M2M Gateway should be able to authenticate the M2M Service Capabilities or M2M Applications from which request is received.
- The M2M System should support a security solution that makes it impossible to acquire information about the data collected by eavesdropping at any point in the network. A particular application may or may not require the use of such security solution. Security solution should not prevent regulatory requirements such as lawful interception.
- End points of the M2M System should be able to verify the integrity of the data exchanged.
- The M2M System should support mutual authentication and authorization between the end-user and the application or capability in the M2M service layer.
- M2M devices that require device integrity validation should provide a trusted execution environment. The Trusted Environment (TrE) should be a logical entity which provides a trustworthy environment for the execution of sensitive functions and the storage of sensitive data. All data produced through execution of functions within the TrE should be unknowable to unauthorized external entities. The TrE should perform sensitive functions (such as storing secret keys and providing cryptographic calculations using those secret keys) needed to perform M2M device integrity check and device validation.

5.2.13.6 Use case source

ESMIG, Document: Smart Metering Functionality Use Cases, ESMCR003-002-1.0, October 2009 [i.4].

5.2.14 Interact with Devices at the Premise

5.2.14.1 General Use Case Description

This High Level Use Case is aligned to the "Additional Functionality" F5 described in clause 4.1.
It describes how the Smart Metering Information System interacts with other Smart devices at the premise. It includes the provision of information to these devices and the management of that relationship via configuration and appropriate communication links.
The Consumer can choose to approve or decline these interactions with the Smart device(s) as necessary. Smart devices at a premise may include thermostats or appliances with a high consumption.

NOTE: Smart devices refer to devices or appliances which are installed and configured at the Consumer's premise to interact with the Smart Metering Information System.

5.2.14.2 Stakeholders

Consumer, Asset Entity, Bill Entity.

5.2.14.3 Scenario

Pre Conditions:

The Smart Metering Information System is installed and configured.
The Smart Metering Information System recognises the Asset Entity and/or Bill Entity and has an address for them.
Smart devices are already installed and configured at the premise for the Smart Metering Information System to interact with and they are able to interact with them.

Post Conditions:

The Smart Metering Information System confirms to the Asset Entity and/or Bill Entity (or another authorised party providing services) that an interaction with Smart devices has been completed.
The Asset Entity and/or Bill Entity are aware that a failure has occurred.

Trigger:

The Smart Metering Information System receives an instruction to interact with the Smart devices or a defined point in its parameter/schedule is reached for it to interact with the Smart device.

5.2.14.4 Information Exchanges

Basic Flow:

1) The Smart Metering Information System receives an instruction from the Asset Entity and/or Bill Entity to interact with the Smart devices or a defined point in the parameter/schedule is reached for an interaction to occur.

2) The Smart Metering Information System updates the Consumer's display with the interaction details.

3) The Consumer approves or declines the interaction details.

4) The Smart Metering Information System sends a message to the Asset Entity and/or Bill Entity confirming that the Consumer has accepted or declined the interaction.

Alternative Flow:

At Basic Flow step 2:

1) The Smart Metering Information System deems the message invalid.

2) The Smart Metering Information System sends notification to the Asset Entity and/or Bill Entity detailing error type along with date/time stamp.

or

1) The Smart Metering Information System fails to instigate an interaction as per defined parameter/schedule.

2) The Asset Entity and/or Bill Entity is aware that a failure has occurred.

At Basic Flow step 4:

1) The Asset Entity and/or Bill Entity fail to receive a message from the Smart Metering Information System confirming whether the Consumer has decided to approve or decline the interaction.

2) The Asset Entity and/or Bill Entity is aware that a failure has occurred.

5.2.14.5 Potential new requirements

- The M2M System should support accurate and secure time synchronisation. M2M Devices and M2M Gateways may support time synchronization or secure time synchronisation.
- M2M Application should be able to specify a periodic reporting of specific parameters for a specific M2M Device or group of M2M Devices. The M2M Application should be able to modify the value of the requested time period.
  In addition to the periodic reporting mechanism, M2M Application should be able to request the same report to the same M2M Device or group of M2M Devices in an on-demand mode.
- The M2M System should support the capability to remotely change the state of a M2M Device e.g. enable or disable.
- The M2M System should support transaction handling between cooperating objects capable of handling this functionality.
- The M2M System should support the following mechanisms for receiving information from M2M Devices and M2M Gateways:
  - Receiving unsolicited information (passive retrieval).
  - Receiving scheduled information.
  - Operating particular algorithms for retrieving information (e.g., round robin, random within given time window, round robin groups with random reply in given time window).
- An object may be able to communicate in a peer-to-peer manner with any other connected object. In this case, packet flows should be supported between these objects.
- The M2M System should be able to authenticate the M2M Device or M2M Gateway. For M2M Devices supporting authentication and connected via an M2M Gateway, the authentication may be performed directly to the M2M System or to the authenticated M2M Gateway.
- When there is a request for data or device access, the M2M Device or M2M Gateway should be able to authenticate the M2M Service Capabilities or M2M Applications from which request is received.
- The M2M System should support a security solution that makes it impossible to acquire information about the data collected by eavesdropping at any point in the network. A particular application may or may not require the use of such security solution. Security solution should not prevent regulatory requirements such as lawful interception.
- End points of the M2M System should be able to verify the integrity of the data exchanged.
- The M2M System should support mutual authentication and authorization between the end-user and the application or capability in the M2M service layer.
- M2M devices that require device integrity validation should provide a trusted execution environment. The Trusted Environment (TrE) should be a logical entity which provides a trustworthy environment for the execution of sensitive functions and the storage of sensitive data. All data produced through execution of functions within the TrE should be unknowable to unauthorized external entities. The TrE should perform sensitive functions (such as storing secret keys and providing cryptographic calculations using those secret keys) needed to perform M2M device integrity check and device validation.

5.2.14.6 Use case source

ESMIG, Document: Smart Metering Functionality Use Cases, ESMCR003-002-1.0, October 2009 [i.4].

5.2.15 Manage Efficiency Measures at the Premise using Smart Metering Information System Data

5.2.15.1 General Use Case Description

This High Level Use Case is aligned to the "Additional Functionality" F6 described in clause 4.1.
It describes how the Smart Metering Information System provides the Efficiency and/or the Consumer with data that allows the Consumer to make informed choices relating to consumption at the premise.
The Efficiency Entity instigates measures to improve efficiency or proposes measures for improving efficiency for the Consumer. The Consumer is able to approve or decline these measures.

5.2.15.2 Stakeholders

Efficiency Entity, Consumer.

5.2.15.3 Scenario

Pre Conditions:

The Smart Metering Information System is installed and configured.
The Smart Metering Information System recognises the Efficiency Entity and has an address for it.

Post Conditions:

The Efficiency Entity receives notification from the Smart Metering Information System that an efficiency measure has been actioned.
The Efficiency Entity receives notification from the Smart Metering Information System that the Consumer has declined to action an efficiency measure.

Trigger:

The Efficiency Entity decides to instigate/propose an efficiency measure.

5.2.15.4 Information Exchanges

Basic Flow:

1) The Efficiency Entity sends a message to the Smart Metering Information System to instigate/propose an efficiency measure.

2) The Smart Metering Information System validates the message.

3) The Smart Metering Information System updates the Consumer's display with the message.

4) The Consumer approves or declines the message.

5) The Smart Metering Information System sends a message to the Efficiency Entity confirming the action that has been carried out.

Alternative Flow:

At Basic Flow step 2:

1) The Smart Metering Information System deems the message invalid.

2) The Smart Metering Information System sends notification to the Efficiency Entity detailing error type along with date/time stamp.

At Basic Flow step 5:

1) The Efficiency Entity does not receive a message from the Smart Metering Information System confirming what action has been taken by the Consumer.

2) The Efficiency Entity is aware that a failure has occurred.

5.2.15.5 Potential new requirements

- The M2M System should support accurate and secure time synchronisation. M2M Devices and M2M Gateways may support time synchronization or secure time synchronisation.

- M2M Application should be able to specify a periodic reporting of specific parameters for a specific M2M Device or group of M2M Devices. The M2M Application should be able to modify the value of the requested time period.
  In addition to the periodic reporting mechanism, M2M Application should be able to request the same report to the same M2M Device or group of M2M Devices in an on-demand mode.

- The M2M System should support the capability to remotely change the state of a M2M Device e.g. enable or disable.

- The M2M System should support transaction handling between cooperating objects capable of handling this functionality.

- The M2M System should support the following mechanisms for receiving information from M2M Devices and M2M Gateways:

  - Receiving unsolicited information (passive retrieval).

  - Receiving scheduled information.

  - Operating particular algorithms for retrieving information (e.g., round robin, random within given time window, round robin groups with random reply in given time window).

- An object may be able to communicate in a peer-to-peer manner with any other connected object. In this case, packet flows should be supported between these objects.

- The M2M System should be able to authenticate the M2M Device or M2M Gateway. For M2M Devices supporting authentication and connected via an M2M Gateway, the authentication may be performed directly to the M2M System or to the authenticated M2M Gateway.

- When there is a request for data or device access, the M2M Device or M2M Gateway should be able to authenticate the M2M Service Capabilities or M2M Applications from which request is received.

- The M2M System should support a security solution that makes it impossible to acquire information about the data collected by eavesdropping at any point in the network. A particular application may or may not require the use of such security solution. Security solution should not prevent regulatory requirements such as lawful interception.

- End points of the M2M System should be able to verify the integrity of the data exchanged.

- The M2M System should support mutual authentication and authorization between the end-user and the application or capability in the M2M service layer.

- M2M devices that require device integrity validation should provide a trusted execution environment. The Trusted Environment (TrE) should be a logical entity which provides a trustworthy environment for the execution of sensitive functions and the storage of sensitive data. All data produced through execution of functions within the TrE should be unknowable to unauthorized external entities. The TrE should perform sensitive functions (such as storing secret keys and providing cryptographic calculations using those secret keys) needed to perform M2M device integrity check and device validation.

5.2.15.6 Use case source

ESMIG, Document: Smart Metering Functionality Use Cases, ESMCR003-002-1.0, October 2009 [i.4].

5.2.16 Display Messages

5.2.16.1 General Use Case Description

This High Level Use Case is aligned to the "Additional Functionality" F6 described in clause 4.1.
It describes how the Smart Metering Information System receives, validates and displays messages from the Bill Entity and/or Energy Services Provider and/or the Efficiency Entity. These messages for the Consumer may include advice relating to the supply, advance notifications, generic information or for marketing purposes. The Consumer is able to approve or decline these messages.

5.2.16.2 Stakeholders

Consumer, Bill Entity, Efficiency Entity, Energy Services Provider.

5.2.16.3 Scenario

Pre Conditions:

The Smart Metering Information System is installed and configured.
The Smart Metering Information System recognises the Bill Entity and/or Energy Services Provider and/or Efficiency Entity and has an address for them.

Post Conditions:

The Smart Metering Information System confirms to the Bill Entity and/or Energy Services Provider and/or Efficiency Entity that a message has been approved or declined by the Consumer.
The Bill Entity and/or Energy Services Provider and/or Efficiency Entity is aware when a failure has occurred.

Trigger:

The Bill Entity and/or Energy Services Provider and/or Efficiency Entity decide to send an instruction to the Smart Metering Information System to display a message for the Consumer.

5.2.16.4 Information Exchanges

Basic Flow:

1) The Bill Entity and/or Energy Services Provider and/or Efficiency Entity send an instruction to the Smart Metering Information System to display a message for the Consumer.

2) The Smart Metering Information System validates the request.

3) The Smart Metering Information System displays the message for the Consumer.

4) The Consumer approves or declines the message.

5) The Smart Metering Information System sends a message to the Bill Entity and/or Energy Services Provider and/or Efficiency Entity confirming the Consumer's action.

Alternative Flow:

At Basic Flow step 2:

1) The Smart Metering Information System deems the request invalid.

2) The Smart Metering Information System sends notification to the Bill Entity and/or Energy Services Provider and/or Efficiency Entity detailing error type along with date/time stamp.

At Basic Flow step 5:

1) The Bill Entity and/or Energy Services Provider and/or Efficiency Entity does not receive a message from the Smart Metering Information System confirming the Consumer's action.

2) The Bill Entity and/or Energy Services Provider and/or Efficiency is aware that a failure has occurred.

5.2.16.5 Potential new requirements

- The M2M System should support accurate and secure time synchronisation. M2M Devices and M2M Gateways may support time synchronization or secure time synchronisation.
- M2M Application should be able to specify a periodic reporting of specific parameters for a specific M2M Device or group of M2M Devices. The M2M Application should be able to modify the value of the requested time period.
  In addition to the periodic reporting mechanism, M2M Application should be able to request the same report to the same M2M Device or group of M2M Devices in an on-demand mode.
- The M2M System should support the capability to remotely change the state of a M2M Device e.g. enable or disable.
- The M2M System should support transaction handling between cooperating objects capable of handling this functionality.
- The M2M System should support the following mechanisms for receiving information from M2M Devices and M2M Gateways:
  - Receiving unsolicited information (passive retrieval).
  - Receiving scheduled information.
  - Operating particular algorithms for retrieving information (e.g., round robin, random within given time window, round robin groups with random reply in given time window).
- An object may be able to communicate in a peer-to-peer manner with any other connected object. In this case, packet flows should be supported between these objects.
- The M2M System should be able to authenticate the M2M Device or M2M Gateway. For M2M Devices supporting authentication and connected via an M2M Gateway, the authentication may be performed directly to the M2M System or to the authenticated M2M Gateway.
- When there is a request for data or device access, the M2M Device or M2M Gateway should be able to authenticate the M2M Service Capabilities or M2M Applications from which request is received.
- The M2M System should support a security solution that makes it impossible to acquire information about the data collected by eavesdropping at any point in the network. A particular application may or may not require the use of such security solution. Security solution should not prevent regulatory requirements such as lawful interception.
- End points of the M2M System should be able to verify the integrity of the data exchanged.
- The M2M System should support mutual authentication and authorization between the end-user and the application or capability in the M2M service layer.
- M2M devices that require device integrity validation should provide a trusted execution environment. The Trusted Environment (TrE) should be a logical entity which provides a trustworthy environment for the execution of sensitive functions and the storage of sensitive data. All data produced through execution of functions within the TrE should be unknowable to unauthorized external entities. The TrE should perform sensitive functions (such as storing secret keys and providing cryptographic calculations using those secret keys) needed to perform M2M device integrity check and device validation.

5.2.16.6 Use case source

ESMIG, Document: Smart Metering Functionality Use Cases, ESMCR003-002-1.0, October 2009 [i.4].

History

Document history		
V1.1.1	May 2010	Publication