

Functional reference architecture for communications in smart metering systems

National foreword

This Published Document is the UK implementation of CEN/CLC/ETSI/TR 50572:2011.

The UK participation in its preparation was entrusted to Technical Committee SMG/1, Smart Meter Group.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2012

Published by BSI Standards Limited 2012

ISBN 978 0 580 76375 5

ICS 33.200; 91.140.01

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 29 February 2012.

Amendments issued since publication

Amd. No.	Date	Text affected
----------	------	---------------

TECHNICAL REPORT

**CEN/CLC/ETSI/TR
50572**

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

December 2011

ICS 33.200; 91.140.01

English version

Functional reference architecture for communications in smart metering systems

Architecture fonctionnelle de référence
pour les communications dans les
systèmes de comptage intelligent

Funktionale Referenzarchitektur für die
Kommunikation in intelligenten
Messsystemen

This Technical Report was approved by CEN and CENELEC on 2011-12-01.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.



CEN-CENELEC
Management Centre:
Avenue Marnix 17, B-1000
Brussels



CEN-CENELEC
Management Centre:
Avenue Marnix 17, B-1000
Brussels



ETSI Secretariat
650, Route des Lucioles
06921 Sophia-Antipolis Cedex
France

Contents

Page

Foreword	4
Introduction	5
1 Scope	5
2 Legislative framework	6
2.1 Directives	6
2.2 Metrological considerations	6
2.3 References	7
3 Commonly used terms	7
4 Approach to standardization	12
4.1 Principles	12
4.2 Scope of standardization work	12
4.3 Smart metering in the context of smart grids	13
5 Privacy and data security	14
5.1 Introduction	14
5.2 Privacy and data protection	14
5.2.1 Legislative framework	14
5.2.2 Approach	15
5.3 General security policy and concepts	15
5.3.1 Principles	15
5.3.2 Security concept	16
5.3.3 Tamper resistance	17
5.3.4 Security policy	17
6 Architecture and configurations	17
6.1 Introduction	17
6.2 Scope of architecture	17
6.3 Functional reference architecture	18
6.4 Physical configurations	20
6.5 Description of functional entities	20
6.5.1 Introduction	20
6.5.2 Central communication system / AMI Head End System (HES)	20
6.5.3 Local Network Access Point (LNAP)	20
6.5.4 Neighborhood Network Access Point (NNAP)	21
6.5.5 Metering end devices	21
6.5.6 Display and home automation	22
6.6 Interfaces	22
6.6.1 Introduction	22
6.6.2 AMI Head End System interface (G interface)	22
6.6.3 NNAP interface (C interface)	22
6.6.4 Metering end device interface (M interface)	22
6.6.5 Display and home automation end device interfaces (H1, H2 and H3 interfaces)	23
6.6.6 LNAP / NNAP Peer Interfaces (L and N interfaces)	23
7 Standardization overview and co-ordination between the ESOs	23
8 Currently available communications standards and further standardization	24
8.1 Introduction	24
8.2 Table of existing communications standards and standards to be developed under the mandate	25
8.3 Product standards related to additional functionalities	41
9 Interoperability and conformance	41
9.1 Interoperability	41
9.1.1 Principles	41
9.1.2 Interface standards	41
9.2 Conformance and interoperability testing	42
9.2.1 Conformance testing	42
9.2.2 Interoperability testing	42

Annex A (informative) SM-CG use cases .	43
A.1 Introduction .	43
A.2 Methodology .	43
A.3 Table of use cases .	44
Annex B (informative) Abbreviations and glossary of commonly used terms in smart metering .	49
B.1 List of abbreviations .	49
B.2 Glossary of commonly used terms - sources .	51
B.3 Glossary of commonly used terms .	52
Annex C (informative) Functional reference architecture for smart metering communications and configuration examples .	63
Annex D (informative) Product standards related to additional functionalities .	67
Annex E (informative) History .	69
Figures	
Figure 1 — Smart metering in the context of smart grid and home automation .	14
Figure 2 — Reference architecture diagram for smart metering communications .	18
Figure 3 — Responsibilities for interface standardization co-ordination, in co-operation with other TCs .	23
Figure 4 — The principle of conformance testing .	42
Figure 5 — The principle of interoperability testing .	42
Figure C.1 — Functional reference architecture for smart metering communications - as shown in 6.3, Figure 2 .	63
Figure C.2 — Configuration example (i) – no neighborhood network .	64
Figure C.3 — Configuration example (ii) – no local network .	65
Figure C.4 — Configuration example (iii) – Multiple meter communications via LNAP .	66
Tables	
Table 1 — Existing communications standards and standards to be developed under the mandate .	25
Table A.1 — Use cases .	44

Foreword

This document (CEN/CLC/ETSI/TR 50572:2011) has been prepared by CEN/CENELEC/ETSI Smart Meters Coordination Group (SM-CG).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under Mandate M/441 given to CEN, CENELEC and ETSI by the European Commission and the European Free Trade Association.

Introduction

This Technical Report identifies a functional reference architecture for communications relevant for smart metering systems and the standards relevant to meeting the technical / data communications requirements of Mandate M/441, in particular to assist the active participation of consumers in the energy markets. The architecture has been developed drawing on existing and planned implementations but its generic nature should enable it to support future different implementations.

Clause 1 sets out the scope of this Technical Report on communications in the context of the overall standardization work being undertaken in response to Mandate M/441, including that on additional functionalities.

Clause 2 gives the legislative framework and lists the references underpinning the smart metering work more generally. Clause 3 provides relevant extracts from the glossary of commonly used terms developed to support the M/441 Mandate work.

For the benefit of stakeholders including the European Commission, Clause 4 then sets the standardization work on communications in the context of the overall approach to the M/441 Mandate, with particular reference to the link between smart metering and smart grids.

Clause 5 considers privacy and data security.

Clause 6 ("Architecture") presents a functional reference architecture for smart metering systems, identifying the functional entities and interfaces that the communications standards should address. Clause 7 gives a general overview of the co-ordination between the ESOs for each of the specified interfaces.

Clause 8 ("Currently available communications standards and further standardization") provides a table setting out current and future communications standards which are considered to be relevant for smart metering in Europe.

The table (shown in 8.2) indicates the most relevant current standards together with the communications standards to be developed in the course of the mandate and the ESO technical committee responsible for co-ordinating the standardization work. It also identifies the smart metering interfaces addressed by the standards noted. The table is not meant to be an exhaustive list of standards; other alternative standards will be considered in the future and could be determined to be acceptable standards as well.

Clause 9 ("Interoperability and conformance") considers the nature of interoperability required under M/441 and responsibilities for conformance testing.

Annexes are included, to assist understanding of the use cases envisaged and terms used, give examples of practical implementations of the architecture described and to identify relevant product standards.

1 Scope

This Technical Report concerns the following communications deliverable within M/441:

A European standard comprising a software and hardware open architecture for utility meters that supports secure bidirectional communication upstream and downstream through standardized interfaces and data exchange formats and allows advanced information and management and control systems for consumers and service suppliers.

The architecture must be scalable to support from the simplest to the most complex applications.

Furthermore, the architecture must consider current relevant communications media and be adaptable for future communication media.

The communication standard of the open architecture must allow the secure interfacing for data exchanges with the protected metrological block.

Since no single standard can cover all aspects for the full application range of smart metering systems, the deliverable takes the form of this Technical Report.

The Technical Report is the second document produced by the Smart Metering Co-ordination Group following acceptance of the Mandate 441 (M/441). The first - a response to the mandate - was issued in December 2009 and provided an overview of the current and future standardization activities, considering both the communications and the additional functionalities of smart meters.

Once the standardization activity undertaken in response to Mandate M/441 is complete for both the communications and additional functionality aspects, a final report will be produced providing a list of the finalized standards in both these areas.

2 Legislative framework

2.1 Directives

The Energy Services Directive (2006/32/EC) and the recently adopted electricity and gas directives (2009/72/EC and 2009/73/EC) are important elements in the background to the M/441 Mandate.

For electricity, the directive requires the implementation of *'intelligent metering systems that shall assist the active participation of consumers in the ... market'*. Such systems must be in place for 80 % of electricity consumers by the end of 2020 (unless an economic assessment shows that a lower figure is appropriate).

For gas, there may be an economic assessment of such metering systems (by September 2012) but there is no specific target date by which they have to be installed, although this should be achieved within a reasonable period of time.

The number of electricity and gas meters potentially required to be replaced over the coming decade makes this standardization work urgent.

In the water sector, smart metering may contribute to meeting the goals of the Water Framework Directive (2000/60/EC), by allowing better control of water uses by consumers. It may also help implementation of the action plan being currently finalized against water scarcity and the impact of droughts, notably regarding "water performances of buildings".

2.2 Metrological considerations

The Measuring Instruments Directive 2004/22/EC (MID) covers the essential (metrological) requirements of meters and is currently being reviewed in the context of the adoption of the New Legislative Framework 765/2008/EC. The European Commission is now in the process of preparing a report on the implementation of the MID, for submission to the European Parliament and Council. See: http://ec.europa.eu/enterprise/sectors/legal-metrology-and-prepack/public-consultation/index_en.htm

Smart meter standardization undertaken in response to M/441 deals with additional functionalities not of a metrological nature which are not prohibited by the MID provided they do not affect the metrology required by the MID.

Consideration should be given at the design stage of any smart metering system to such functions as real-time clocks or tariff schedule registers which may need to be synchronized through external communication. This is to ensure that the metrological characteristics of the meter are not influenced in any inadmissible way by the connection to it of another device, by any feature of the connected device itself or by any remote device that communicates with the meter.

WELMEC has produced Guidelines which set out recommendations for the software used in or connected to the metrologically protected part of measuring instruments and its communications interface(s). The standards to be developed under M/441 should consider these recommendations, in particular concerning the functional requirement of upgrading software / firmware and specific provisions regarding the downloading of legally relevant and non-legally relevant software. Care should be taken at the design stage to ensure that any software / firmware upgrade process does not influence those parts of the meter that are under the control of the MID.

2.3 References

- 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.
- Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC
- Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC
- Directive 2000/60/EC of the European Parliament and of the Council of 23 October 2000 establishing a framework for the Community action in the field of water policy.
- Directive 2004/22/EC of the European Parliament and of the Council of 31 March 2004 on Measuring Instruments.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

3 Commonly used terms

Many terms used in this document are explained in the standalone glossary of terms commonly used in smart metering, appended to this report. Relevant extracts are given below. In this document, these are marked in *cursive* letters when they first appear.

NOTE The glossary does not supersede more detailed definitions used or to be developed by ESOs.

3.1

additional functionality

function that a smart metering system provides over and above the metrological functions covered by the Measuring Instruments Directive

3.2

architecture

structure and behavior of the technology infrastructure of an enterprise, solution or system

NOTE 1 Functional architecture can be viewed as the set of basic information processing capabilities available to an information processing system.

NOTE 2 Software architecture of a program or computing system is the structure or structures of the system, which comprise software components, the externally visible properties of those components, and the relationships between them.

NOTE 3 Hardware architecture refers to the identification of a system's physical components and their interrelationships.

3.3

Advanced Metering Infrastructure

AMI

infrastructure which allows two way communications between the Head-End System and the meter(s) and may be linked to other in-house devices

3.4

Automated Meter Management

AMM

also called Advanced Metering Management. Refers to smart metering actions requiring communication, for example, remote actions. AMM directly incorporates additional functionalities beyond AMR

3.5

Automatic Meter Reading

AMR

technology for remotely obtaining metering data from an on-site meter by communication from an access point outside the premises.

AMR technologies include handheld, mobile or fixed network technologies based on telephony platforms (wired and wireless), radio frequency (RF), or Power Line Carrier (PLC)

3.6

(data) concentrator

intelligent station in a hierarchical communications network where incoming data (generated by multiple meters) is processed as appropriate and then repackaged, relayed, retransmitted, discarded, responded to, consolidated, prioritized and / or increased to multiple messages

3.7

conformance

fulfillment of a product, process or service of specified requirements

3.8

consumer

end user of electricity, gas, water or heat

NOTE 1 The Meter Data Collector (and when applicable also the consumer's supplier) may communicate with the consumer through the *AMI*.

NOTE 2 As the consumer can also generate energy using a Distributed Energy Resource, he is sometimes called the "Prosumer".

3.9

Companion Specification for Energy Metering

COSEM

interface model for communicating with energy metering equipment, providing a view of the functionality available through the communication interfaces

NOTE The modeling uses an object oriented approach.

3.10

customer

purchaser and/or user of a product or service supplied by an organization. The "Customer" may be the ultimate consumer, user, beneficiary or purchaser

NOTE In the context of Smart Metering the Customer is the same person as the Consumer.

3.11

data security

prevention of one or more of the following:

- a) unauthorized access to information within a data stream;
- b) unauthorized alteration of information within a data stream;
- c) unauthorized generation of messages which could be taken as valid by the receiving equipment
- d) denial of service

See also '**Security**'

3.12

disconnection

removal of supply from a consumer's premises by physical disconnection of the supply

NOTE Reconnection is the reverse operation i.e. restoration of supply.

3.13

distributed generation

electricity generation from multiple small energy sources thus allowing more efficient energy distribution

NOTE Energy is generated closer to the point of consumption, thus reducing network losses.

3.14

Device Language Message Specification

DLMS

ISO-OSI Application Layer specification, independent of the lower layers and thus of the communication channel, designed to support messaging to and from (energy) distribution devices in a computer-integrated environment

NOTE DLMS is specified in EN 62056-53 and is an evolution of the Distribution Line Message Specification specified in EN 61334-4-41.

3.15

gateway

device that fully implements the ISO-OSI model for all layers and is used to convert data protocols between different communication systems and standards

NOTE Gateways work on all seven layers of ISO-OSI architecture. The main job of a gateway is to convert protocols between communications networks.

3.16

Hand-Held Unit

HHU

portable device for reading and programming equipment or meters at the consumer's premises or at the access point

NOTE Also known as Hand-held Terminal Unit.

3.17

Home and Building Electronic System

HBES

system for the integration of control applications and the control and management aspects of other applications within a domestic or building environment, including gateways to different transmission media and public networks

3.18

Head End System

HES

central Data System exchanging data via the AMI of various meters in its service area

NOTE it communicates via a WAN directly to the meters via NNAPs and LNAPs.

3.19

Home Area Network

HAN

in-house LN which interconnects domestic equipment and can be used for energy management purposes

NOTE There can be multiple HANs inside a customer's premises.

3.20

index

for gas and water metering, the current reading of the total volume (mass) passed through the meter

3.21

interface

point or means of interaction between two systems

3.22

interoperability

ability of a system to exchange data with other systems of different types and/or from different manufacturers

3.23

load balancing

ability to use network information and/or on-site intelligence to reconfigure distribution networks or to limit customer loads to maintain desired levels of service and improve the utilization of assets

3.24

load limitation

restricted capacity / energy flow resulting in self-disconnection of supply by the meter if the defined threshold was exceeded

3.25

local network

data communication network providing access to local (in-house/building) devices and / or other local networks

3.26

meter

instrument for measuring, memorizing and displaying the consumption of a commodity

3.27

M-bus (meter bus)

a communication standard (wired or wireless) for data exchange with end devices, including, but not limited to utility meters

3.28

meter data

meter readings that allow calculation of the quantity of electricity, gas, water or heat consumed over a period. Meter data thus may include daily and monthly meter readings, interval readings and actual meter register values.

Other readings and data may also be included (such as quality data, events and alarms)

3.29

Meter Operator

MO

entity which offers services on a contractual basis to provide, install and maintain metering equipment related to a supply

3.30

metering end device

combination of the following meter-related functions from the reference architecture:

- metrology functions including the conventional meter display (register or index);
- one or more additional functions. These may also make use of the display;
- meter communication functions

3.31

M2M gateway

entity associated with a Meter, Data Concentrator and/or central system providing M2M service capabilities and a data path to these entities

3.32

neighborhood network

data communication network providing access to several premises and / or other neighborhood networks

3.33

OBject Identification System

OBIS

system defining identification codes for commonly used data items in metering and other equipment

NOTE specified in EN 62056-61 for electricity meters, in EN 13757-1 for non-electricity meters.

3.34

Open Systems Interconnection

OSI

framework for communications processes, defined by ISO, in which the process is divided into seven functional layers, arranged vertically with each having separate and defined responsibility. Each layer communicates only with the layer immediately above and below

3.35

Power Line Carrier

PLC

communications technique using high frequency signals to transmit data over (high voltage) transmission lines transporting electrical power

NOTE In practice the term PLC is also used for communication over distribution lines (low-voltage PLC).

3.36

privacy

safeguarding of personal data

NOTE Personal data is defined by Directive 95/46/EC as 'any information relating to an identified or identifiable natural person.'

3.37

protocol

rules for communication system operation that must be followed if communication is to be effected. Protocols cover one or more layers of the OSI model

3.38

register

Indication of the specific section in the memory of the control and metering unit that records data as determined by the programme in the unit

NOTE The meter can have more than one register.

3.39

security

measures that protect and defend information and information systems by assuring their confidentiality, integrity, access controls, availability and accuracy

See also 'Data Security'

3.40

smart grid

supply network (principally electricity network) that intelligently integrates the behavior and actions of all users connected to it – generators, consumers and those that do both – in order to efficiently ensure a more sustainable, economic and secure electricity supply

3.41

smart meter

meter with additional functionalities one of which is data communication

3.42

smart metering system

system comprising metering end device, HES and their communication infrastructure (AMI)

3.43

supplier

entity that offers contracts for supply to a consumer (the supply contract) and bills the consumers for consumption

NOTE In some countries referred to as Retailer.

3.44

tariff

price structure (normally comprising a set of one or more rates of charge) applied to the consumption of a product or service provided to a consumer

3.45

use case

description of the interaction between one or more actors, represented as a sequence of simple steps

NOTE 1 Actors are entities that exist outside the system ('black box') under study, and which take part in a sequence of activities in a dialogue with the system to achieve a specific goal. Actors may be end users, other systems, or hardware devices.

NOTE 2 Each Use Case is a complete series of events, described from the point of view of the actor.

3.46

Wide Area Network

WAN

extended data communication network connecting a large number of communication devices over a large geographical area

4 Approach to standardization

4.1 Principles

As noted in Clause 5 of the SM-CG report in December 2009, the goal is to facilitate harmonized solutions through appropriate voluntary standards. Member States will then be able to specify their own requirements within such a harmonized framework, taking account of national legislation and specific local considerations.

The European Standards Organizations will first assess the suitability of international, European and national standards and will give preference to (draft) European and international standards. If no suitable standard is available for any specific part of the smart metering system, the ESO shall identify the gap between the existing standard(s) and the required standard(s), considering national proposals where useful, and then work to improve these standard(s) and/or develop new ones where needed. Technical committees will seek co-operation with other relevant fora and consortia.

The relevant technical committees are strongly encouraged to accept new work items at any time when required (subject to ESO rules), in order to ensure that new technologies can be adopted from the market and incorporated into the standardization process.

4.2 Scope of standardization work

The future standardization work focuses on meeting the needs of the residential (household) and small and medium enterprise (SME) sectors. This corresponds to the focus of M/441 and the need to improve consumers' awareness of their energy and water usage (hereinafter "consumption").

In order to ensure suitable communications standards to support the development of smart metering systems, the standardization described in this report will take account of the following six broad areas of *additional functionality*, closely based on those identified in the SMCG report of December 2009:

- **Functionality 1: Remote reading of metrological register(s) and provision to designated market organizations;**
- **Functionality 2: Two-way communication between the metering system and designated market organization(s)¹;**
- **Functionality 3: To support advanced tariffing and payment systems;**
- **Functionality 4: To allow remote disablement and enablement of supply and flow / power limitation;**
- **Functionality 5: To provide secure communication enabling the smart meter to export metrological data for display and potential analysis to the end consumer or a third party designated by the end consumer;**
- **Functionality 6: To provide information via web portal/gateway to an in-home/building display or auxiliary equipment.**

This Technical Report on communications considers additional functionalities only to the extent necessary to ensure that there are smart metering communications standards to support the functionalities envisaged.

The smart metering system may be used for a further important functionality:

- **to enable communication of AMI components with devices or gateways within the home / building used in the provision of energy efficiency and demand-side management services.**

In this role it is directly linked to smart grid functionalities using building and home automation systems. Building and home automation are outside the scope of this mandate; however their interfaces with the smart meter will be treated in co-operation with the SM-CG.

¹ This supports additional functions aside from remote reading of metrological registers. Examples are system configuration, collecting supply quality data, managing local generation, detecting tampering, firmware upgrades etc. See also Annex A – Use cases.

Note that the functionalities are services which can be provided via a smart metering system, without excluding the possibility of certain services being provided by means other than via this system.

The list of functionalities should not be seen as a minimum list of smart metering functionalities to be implemented in Europe, since not all functionalities will necessarily feature in all applications or in all Member States and functions outside this list may also be defined.

As required by M/441, smart metering standards should permit a range of approaches – from fully integrated instruments to modular and multi-part solutions. Modular and multi-part installations may require additional interfaces between the constituent parts - these interfaces are considered to be outside the scope of M/441.

As the relevant directives in Clause 2 do not specify essential requirements, the standards identified and/or developed under the M/441 Mandate will not be harmonized under those directives. However this does not preclude the possibility of broad regulatory guidelines in the area of electricity and gas smart metering.

The standards are intended to ensure the provision of a secure and reliable service for consumers and to support services which are generally covered by a wider regulatory or legislative framework, including, for example, privacy, data protection and data security requirements – see Clause 5.

To clarify standardization requirements and to ensure consistency in the smart meter dataflows anticipated, it is helpful to consider these functionalities in greater detail, through use cases. This Technical Report describes in greater detail a variety of use cases related to these broad functionalities. It has to be stressed that it is outside the scope of M/441 to decide on the need for smart metering systems to fulfill any particular use case described.

Use cases can be defined at different levels, depending on their purpose. [Annex A](#) shows how the use cases adopted by SM-CG relate to each of the above functionalities in order to describe how different actors interact with a smart metering system. However this list is illustrative and not final; the SM-CG is carrying out further work on use cases in co-operation with the ESOs.

Technical Committees should therefore take care not to restrict the way in which services can be provided. The use cases are intended to be used to help define functional requirements, which then help determine the nature of the bidirectional (where necessary) upstream and downstream communications required. These thus facilitate the work of technical committees.

In addition to the extract of commonly used terms in Clause 3, a full glossary has been prepared, which is included as [B.3](#).

4.3 Smart metering in the context of smart grids

The work undertaken in response to M/441 considers the high-level smart metering functionalities which are additional to the traditional metrological requirements applying to electricity and other meters. The major focus of the mandated work under M/441 is the provision of improved information and services to consumers and enabling consumers to better manage their consumption.

Particularly in relation to electricity metering, there is the important additional objective of facilitating *smart grid* applications, notably through the incorporation of distributed generation. Electricity smart grid standardization is the subject of Mandate M/490 and is outside the scope of this report. However the M/441 Mandate envisages smart metering as a key enabler for smart grids, providing for two-way information flows between the meter and the designated market organization(s).

Smart metering systems may exist in the context of larger smart grid infrastructures and may co-exist with home automation systems. This is illustrated in Figure 1.

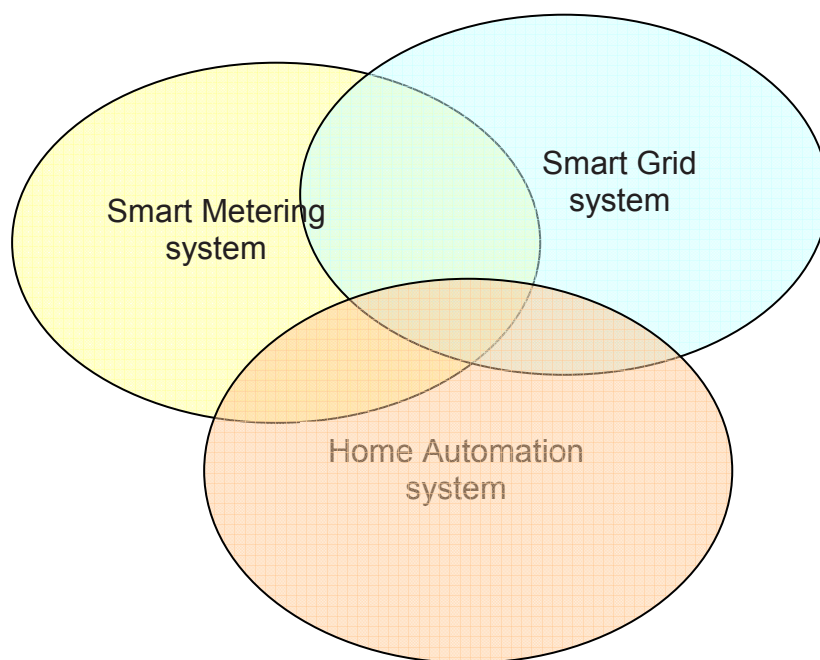


Figure 1 — Smart metering in the context of smart grid and home automation

As noted in 4.2 above, smart metering applications may overlap with applications of smart grid systems and building / home automation systems. The communications infrastructures supporting these applications may be separate or may be usefully shared.

5 Privacy and data security

5.1 Introduction

For public acceptance of smart metering, suitable privacy and data protection safeguards need to be in place so that consumers can be confident that their data is treated securely and their privacy is not infringed. In addition, while traditional metering and control systems in premises may be comparatively less susceptible to security attacks, attention should be given to address the vulnerability of smart metering / smart grid systems. Smart metering products and solutions should therefore be designed from the start with appropriate levels of both privacy and security at their core, and appropriate and scalable solutions found.

As with other aspects of the M/441 standardization work, ESOs are responsible for updating, extending or developing new standards covering the security and data protection aspects of smart metering / smart grid interfaces. Comparing the risks addressed through standards, guidelines and codes of practice in other industries e.g. banking and telecoms already provides a useful basis for what could be appropriate levels of safeguard in highly sensitive areas such as payment data, consumption levels/profiles and connection & disconnection of supply.

5.2 Privacy and data protection

5.2.1 Legislative framework

The present European legal framework regarding privacy and data protection derives from the EU privacy and data protection directives and treaties. The present data protection directive is due to be reviewed.

The purpose, design, functionalities and implementation of any particular smart metering system will to a large extent determine whether or not it will comply with current or future EU privacy and data protection legislation. The review of the data protection directive could therefore make provision for guidelines or codes of practice to be developed in relation to smart metering, complementing EU directives and standards and reflecting the governance and compliance arrangements appropriate for each national and industry situation.

5.2.2 Approach

Smart metering standardization should have regard to this legislation and to future regulatory guidelines or codes of practice which may be developed to support smart metering (and / or smart grids). Privacy requirements should be designed into smart metering communication systems and implementations from the outset and use of effective privacy-enhancing technologies (e.g. cryptography) should be considered – see also 5.3 below.

Standardization should support smart metering deployments by setting a framework to help ensure privacy is appropriately protected. Exact mechanisms to achieve this will have to be determined in relation to each individual implementation.

5.3 General security policy and concepts

5.3.1 Principles

The following principles derived from different areas applicable to data security issues are of importance in considering smart metering configurations:

- security needs to be seen as an end-to-end characteristic encompassing systems, processes and people, and not in terms of individual components;
- security should be designed in at the architectural level, not added later;
- from a systems viewpoint, security of the smart metering infrastructure is linked to security of smart grid and home automation networks;
- security implementation should be scalable in terms of applications and the capability of devices;
- for systems with a long lifetime expectancy such as smart meters, security measures will need to evolve over time as more sophisticated attacks become available;
- cryptographic algorithms provide a wide range of scalable security for systems, sub-systems and components;
- security is a permanent tasks to be maintained as an ongoing process by the operating organization;
- security in smart metering could be seen as ‘cyber security’ in IT systems due to its high affinity in structure, elements and applications;
- smart meters, communication networks and data collector systems should be regularly tested for security vulnerabilities by an independent third party.

Therefore in considering standardization, data security is used more in the sense of ‘cyber security’ and is concerned mainly with securing components (like meters, network access points, etc.) in the overall network with respect to proper system behavior.

Many security considerations are already covered in existing standards and will be taken into account in the development of standards resulting from the M/441 Mandate.

Establishing and executing security policies are outside the scope of the standards to be developed under the M/441 Mandate; however the standards may provide security measures / services supporting those policies e.g. for authentication and encryption. The ESOs will also need to consider the outcome of any future mandate developed in the context of smart grid standardization.

In general security is not a purely technical issue - the foundation for a successful technological solution is an appropriate security policy – see 5.3.4 below.

It is worth mentioning that companies have to balance their efforts in security measures. That will result in scenarios where lesser risks could be accepted as residual risks, and more dangerous scenarios, which should result in measures to recognize, to avoid or to mitigate those risks.

Organizational measures will also apply to the involved parties installing and operating the system, but can only be taken into consideration in this document to a limited extent. This however may play an important role in building the consumer trust required to develop the acceptance of smart meters in the public.

5.3.2 Security concept

A security concept refers mainly to an *architecture* model, which represents data flows between role-based data processing functions.

Requirements for the security concept result from the overall security objectives in combination with the derived security services and best practice.

As additional constraints, legal requirements (e.g. metrology & data privacy) will influence the application of security services to dedicated system elements and their interfaces.

From an overall system view, the top-down process has to map the services to the system components and operational process, not forgetting the supporting management systems for initialization, installation, key management etc.

In detail, there are four major security services to support security objectives. They are all relevant for securing sensitive data such as those related to transactions with customers and billing information. They need to be integrated in the perspective of end-to-end communications within the smart metering system, throughout the Local and Neighborhood Network(s), Local / Neighborhood Access Points and *Wide Area Network*:

<u>Security Service</u>	<u>Security objective</u>
— Integrity	-- prevent modification of information by unauthorized parties
— Authentication	-- determine the true identity of a communication party
— Confidentiality	-- prevent disclosure of information to unauthorized parties
— Non-repudiation	-- ensure that a party cannot repudiate/refute the validity of data

Some further security services may be requested (list not exhaustive):

— Availability	e.g. protection against Denial of Service attacks
	This is particularly critical in the case of smart metering, as availability of the smart metering services themselves and availability of supply to the end consumer should be ensured
— Authorization	
— Access control	
— Auditability	
— Protection from unauthorized intervention	

In addition, as mentioned above, scalability by security classification will help to select the tailored approach for the target system. These security services can be realized with different methods and/or techniques with scalability in their characteristics.

Implications for a system, a sub-system or a device may result from the selection of e.g. using symmetric or asymmetric cryptographic methods. In any case the system security will rely on secret security credentials that need to be preserved throughout the whole chain. The implications of the choice of a cryptographic method on the security management process will require careful evaluation.

5.3.3 Tamper resistance

The security concept presented above addresses functional security, which can be standardized and tested. This approach does not however warrant that sensitive devices or processes will be implemented with sufficient skills to resist attacks using sophisticated means such as simple or differential power analysis to discover secret keys used within cryptographic computations.

This is the scope of tamper resistance, which can be ensured e.g. by means of dedicated protection profiles according to ISO/IEC 15408.

5.3.4 Security policy

Standardization in response to M/441 will address the above aspects in the context of an overall smart grid system.

However security policy in general should address from an organizational viewpoint all constraints on functions, information flow between functions, access by external systems and threats, including software and access to data by third persons. Maintaining proper security policy is essential for organizations manipulating the secret security credentials used to protect a system, including manufacturing plants incorporating the credentials in the devices. Established information management security standards such as the EN 27000 series are relevant in this respect.

Security policy is under the responsibility of organizations according to their business processes. The major elements of a security policy, in combination with rules, will determine the overall security that is achieved.

Security policy defines goals and elements of the system, to be supported by organizational policy and technical implementations of security mechanisms. From the viewpoint of manufacturer and system solution provider, these are not addressed here - the link takes place via guidelines and rules to initiate, implement, operate and maintain the system by the responsible organization(s), including periodic checking, control and adjustment.

6 Architecture and configurations

6.1 Introduction

The main objective of this section is to present a functional reference architecture for smart metering systems so as to provide a consistent baseline for standardization by CEN, CENELEC and ETSI and thus to support the M/441 Mandated work.

There are numerous ways in which this functional architecture can be translated into a physical implementation. Devices and communications interfaces can be configured in differing combinations depending on the solution and application required. While some specific examples of such physical configurations are referred to in the text, this is by way of illustration and is not exhaustive of all the possibilities.

6.2 Scope of architecture

The reference architecture defines the functional entities and communications interfaces in a smart metering system. It is intended to support the development of software and hardware architecture and related standards.

To facilitate *interoperability*, standards should be based on European or international standards and follow the Open System Interconnection (OSI) / IP models as appropriate - see Clause 9 below.

6.3 Functional reference architecture

Smart metering systems comprise all functions, entities and interfaces from the utility smart metering applications to smart metering end devices and / or home automation devices used in a smart metering context.

The scope of the M/441 Mandate with respect to communications is limited to the communication infrastructure between the smart metering *Head End System* and the metering end devices, including all functional entities in between.

Figure 2 below gives a simplified overview of functional entities and interfaces in a smart metering communications network; the boxes correspond to functions that in physical terms can be implemented in a number of different ways. This Technical Report is concerned solely with the communications interfaces depicted in blue in Figure 2; the internal functions and interconnections of the metering end device are outside the scope of this document. The dotted lines H2 and H3 support functionalities 5 and 6 and provide interfaces to support the provision of energy efficiency and demand-side management services.

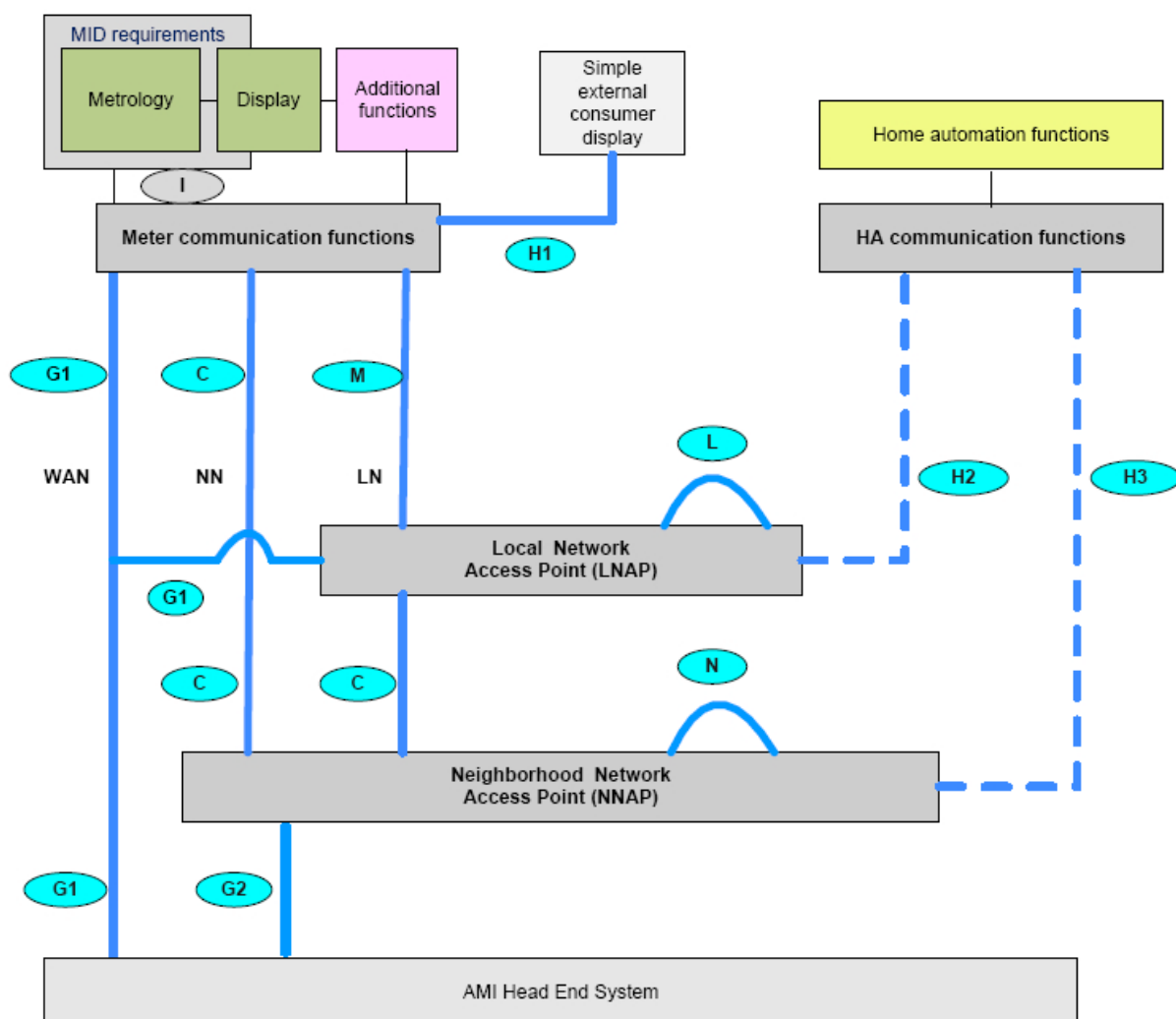


Figure 2 — Reference architecture diagram for smart metering communications

A smart metering system always comprises (a) head end system(s) and metering end devices, together with the communication network between them, which may include

- wide Area Network (WAN) connecting the head end systems to the local systems or networks,
- neighborhood Network (NN) covering a number of premises (optional),
- local Network (LN) within the same premises (optional).

A Neighborhood Network, when present, is accessible through a Neighborhood Network Access Point. Similarly, a Local Network, when present, is accessible through a Local Network Access Point.

Metering end devices may have interfaces to communicate on the LN, the NN or the WAN. These are the M, C and G interfaces respectively and at least one of these should be present.

NOTE 1 The I interface describes the internal link between the metering functions and the communication functions within the metering end device and is outside the scope of the mandate.

A metering end device may have an interface (H1) for a local connection to a simple external consumer display. Home automation end devices (including more advanced displays) may have connections to one or more Network Access Points (H2 & H3).

Access to end devices on the LN is provided by the Local Network Access Point (LNAP). A LNAP has one or more M and H2 interfaces to communicate with the end devices on the LN and one or more C or G interfaces to communicate on the NN and the WAN.

Similarly, access to end devices and to LNAPs on the NN is provided by the Neighborhood Network Access Point (NNAP). A NNAP has a C interface to communicate with entities on the NN and a G interface to communicate through the WAN with the metering head end system(s). It may also have an H3 interface to home automation systems.

Because the Network Access Points (LNAP, NNAP) have to interconnect different networks and may need to translate *protocols*, they contain a gateway function.

The different kinds of metering end devices and display and home automation devices may share a LN or they may have their own LN.

Entities on a given hierarchical level may communicate with each other via an entity at the next higher level.

NOTE 2 An entity at a higher level is generally closer to the head end system.

Additionally, entities at the same level may communicate with other entities at the same hierarchical level.

NOTE 3 This permits network configurations with branched, chained or meshed interconnection, by means of the L and N interfaces (see also 6.6.6 below).

In a practical smart metering system, the reference architecture permits a mix of scenarios to be present. For example:

- some metering end devices may be accessible through the WAN using the G interface;
- some metering end devices may be accessible through the WAN + NN via the C interface; and
- some metering end devices may be accessible through the WAN + NN + LN via the M interface;
- advanced displays and home automation devices may be accessible through the WAN + NN + LN via the H2 or H3 interface.

There are also variations in practice concerning the standards which may be used for the different interfaces. The table in 8.2 indicates for example that while the C interface is used to connect the NNAP and the metering end device or LNAP, in practice standards envisaged for the M interface may be used.

Regardless of the network paths of the specific implementation, special care about security is necessary to prevent unauthorized monitoring or intervention (see also Clause 5: Privacy and data security).

The functional entities and their interfaces are described in more detail in sections 6.5 and 6.6 below.

6.4 Physical configurations

Not all functions will necessarily be present in any physical infrastructure or specific smart metering implementation. Thus, the model in practice does not require there to be devices for each of the above items in a smart metering implementation.

A major physical precondition that the smart metering configuration has to take into account is the impact of the meter's power supply on communication capabilities. As most gas and water meters and related network components are operated on a battery supply basis, where long battery life is generally a key factor, data communication for these components may not be identical to that for mains-powered devices.

The smart metering configuration should accommodate standardization and technological progress.

NOTE Smart metering systems may also employ *Hand Held Units (HHUs)* and *Point Of Sale Terminals (POSTs)*. The interfaces between these and the smart metering system entities are out of the scope of this Technical Report. Human interfaces are similarly out of scope.

6.5 Description of functional entities

6.5.1 Introduction

A functional entity may be implemented in different physical devices depending on the configuration needs.

Each functional entity may have application functions and in order to be able to participate in the system it should have communication functions. The communication functions include the interface handler to manage one or more interfaces.

6.5.2 Central communication system / AMI Head End System (HES)

Central communication systems (AMI Head End Systems) communicate with meters (metering end devices) either directly through the WAN, or using additional Neighborhood Networks via NNAPs and / or Local Networks via LNAPs (collectively NAPs).

HESs are typically part of an *AMR* or *AMM* solution. In terms of the M/441 Mandate, the focus for standardization is limited to the WAN communication part of an *AMR/AMM* system only. Data exchange with other systems e.g. systems for physical meter installation and meter asset management, though of importance to customers, meter operators and suppliers, are beyond the scope of this mandate,

HESs typically manage NAP addresses, *data security* and meter reading pre-processing. In electricity, they provide the top end interface to smart grid functions / applications (the lower-end interface being the NAP function). The interface towards the NAPs is standardized within the M/441 Mandate; the interface from HESs towards central energy and meter data management systems is covered by IEC TC 57 and is considered to be out of the scope of this mandate.

6.5.3 Local Network Access Point (LNAP)

The LNAP is a functional entity that allows access to one or more metering end devices and, when equipped with an H2 interface (interfaces), to advanced display / home automation end devices connected to the LN. A LNAP also may allow data exchange between different functional entities connected to the same LN.

The LNAP may act simply as a router transferring messages between the metering end device and/or display/home automation devices and the NNAP and/or the WAN. Alternatively it may provide a range of services including protocol conversion, device management, security and service capabilities. Services may be provided as functions of the LNAP itself or provide proxy services on behalf of limited capability devices connected to the LN.

The LNAP may also comprise metering application functions. In this case, NNAPs / HES application functions exchange data with the metering application functions implemented in the LNAP and the LNAP application functions exchange data with the functions implemented in the metering / home automation end devices.

LNAP metering application functions may include collecting and retaining data from one or several end devices on a scheduled or on-demand basis, forwarding these data, sending commands etc.

In physical terms, the functional entity LNAP can be realized either as

- an explicit device with physical connections to the meter and / or the LN and the WAN and / or NN,
- an attachment device in the meter (plug-in module), or
- a simple function block inside an integrated meter construction, or
- a mobile device (e.g. hand-held terminal, drive-by).

The LNAP may be used to ensure the local communication of display data and the support of local additional services.

6.5.4 Neighborhood Network Access Point (NNAP)

A NNAP is a functional entity that, when equipped with C interface, allows access to one or more LNAPs or metering end devices and, when equipped with an H3 interface (interfaces), to advanced display / home automation end devices connected to the NN.

A NNAP may also allow data exchange between different functional entities connected to the same NN.

The NNAP communication functions may include NN and end device management, protocol conversion (gateway functionality), security management etc.

The gateway functionality of the NNAP provides a connectivity infrastructure between meters and the central system. It utilizes two separate communication networks. It communicates with the central system via a WAN, and via a NN with the meters and / or LNAPs which it manages. The NNAP is typically used for meter connection in configurations, where a dedicated WAN connection for a single meter / LNAP is not desired.

In addition, the NNAP may also comprise application functions. In this case, HES application functions exchange data with the application functions implemented in the NNAP and the NNAP application functions exchange data with the functions implemented in the LNAPs and/or metering / home automation end devices. NNAP application functions may include collecting and retaining data from one or several end devices and/or LNAPs on a scheduled or on-demand basis, forwarding this data, compressing data, sending commands etc. NNAPs with such application functions are also known as *Data Concentrators*.

6.5.5 Metering end devices

The metering end device is a combination of the following meter-related functions from the reference architecture:

- metrology functions including the conventional meter display (register or index) that are under legal metrological control. When under metrological control, these functions shall meet the essential requirements of the MID;
- one or more additional functions not covered by the MID (see 4.2 above). These may also make use of the display;
- meter communication functions.

The power supply to the metering end device may have bearing on the additional and communication functions. An electricity meter measures electricity consumption / generation and related data. Such meters are mains-powered and the limitations on communications frequency or volumes applicable to battery-powered meters may not apply. However energy usage should not be excessive.

Non-electricity meters, which measure gas, water or heat, are typically battery-powered and this has important implications for the frequency and duration of data communication possible. The location and installation of meters may also be constraining factors. Battery life, which may be subject to national regulation and/or utility purchasing requirements, has to be taken into account in standardization and metering system design, and in the interests of efficiency, provision may need to be made for short communication packets.