# Open Metering System Specification

## Volume 2

## Primary Communication

**Issue 4.0.2 / 2014-01-27**

**RELEASE**

# Document History

| Version | Date | Comment | Editor |
|---|---|---|---|
| 1.0.0 | 2008-06-27 | First final Version | U. Pahl |
| 1.0.1 | 2008-07-01 | Editorial Revision | U. Pahl |
| 1.0.2 | 2008-07-21 | Some format adoptions; table index added; content index limited to structure level 3. | H. Baden |
| 1.0.3 | 2009-02-25 | Correct mistake in Table 10<br>Add changes for 2nd Version | U. Pahl |
| 1.0.4 | 2009-05-13 | Revision in AG1 | AG1 |
| 1.0.5 | 2009-05-30 | Add changes for 2nd Version | U. Pahl |
| 1.0.6 | 2009-06-11 | Update Annex | U. Pahl |
| 1.0.7 | 2009-06-30 | Changes based on protocol#23 | U. Pahl |
| 1.0.8 | 2009-07-03 | Last changes of online review; update Annex A;,L and M, editorial review | U. Pahl |
| 1.0.8 | 2009-07-05 | Editorial and formal review | H. Baden |
| 1.0.9 | 2009-07-17 | Add Time sync frame to MUC-Status, separate ACC-No for M-Bus and wM-Bus | U. Pahl |
| 2.0.0 | 2009-07-20 | Release as V2.0.0 | U. Pahl |
| 2.0.1 | 2010-04-10 | Add Changes for 3rd Version, Add sync Meter transmission; New CI-Fields | U. Pahl |
| 2.0.2 | 2010-11-05 | Add Compact M-Bus Profile; Harmonise Spec. with prEN 13757-3/4 | U. Pahl |
| 2.0.3 | 2010-11-17 | Revision in AG1 | AG1 |
| 2.0.4 | 2010-12-17 | Comments from members of AG1, Bug fix in Annex B | U. Pahl |
| 3.0.0 | 2011-01-21 | Update Changes from Standard revision | U. Pahl |
| 3.0.1 | 2011-01-28 | Editorial Revision. Release as V3.0.1 | U. Pahl / A. Bolder |
| 4.0.0 | 2013-01-10<br>2013-05-06<br>2013-07-02<br>2013-08-19<br>2013-08-30<br>2013-09-24<br>2013-10-20<br>2013-10-21<br>2013-10-23 | New Introduction; Add BSI-support (AFL; new Encryption Mode 7 (dyn. AES) and Mode 13 (TLS); restructure chapters "Supported Device Types" and "Application protocols"; Revision of OBIS-List format; Add new M-Bus Datapoint list, add new section Address handling; Add mandatory support of ELL, Add C-Mode support, Remove obsolete Annex E,F and M; general editorial revision, Add new ext. Annex B, E,F,O and int Annex J; Change Annex A to ext. Annex A; expand rules for ELL-Access number and TPL-Access number Add Timing Diagram fragm. SND-UD | U.Pahl / A. Bolder |
| 4.0.1 | 2014-01-18 | Changes according to Enquiry comments (see OMS_KommentareVol2Issue4_sortiert2_bearbAG1.doc) | U.Pahl |
| 4.0.2 | 2014-01-27 | Add Note to Annex G; Rename VIF-Type to VIB-Type Version 4.0.2 is released | U.Pahl |

# Table of contents

# List of tables

# List of figures

# 1 Introduction

## 1.1 General

This part describes the minimum Open Metering System requirements for the wired and the wireless communication between a slave (meter or an actuator, or breaker) and the (stationary, usually mains powered) master (gateway or other communication unit). It covers the Physical Layer, the Link Layer, the general requirements for communication security (covered in the Authentication and Fragmentation Layer and in the Transport Layer) and the application itself. The Application Layer is focused on the M-Bus protocol. But it also supports the DLMS/COSEM protocol and an SML-based protocol. Detailed information about the required values and the time resolution are given. The total system overview is covered in Volume 1 of the Open Metering System specification (OMSS).[1]

An overall glossary with definitions and abbreviations is provided as separate Annex of Volume 1 of the Open Metering System Specification (general part).

The list of referenced standards and documents (marked with square brackets (like [EN 13757-3:2013]) are listed in the Open Metering System Specification (general part).

Note that according to the language use of standards statements with a “shall” describe mandatory requirements. Statements with a “should” describe recommendations.

This part concentrates on the requirements for basic meters but also includes some optional enhancements for sophisticated meters. This specification supports both mains powered devices (e.g. electricity meters or actuators) and battery driven devices (e.g. water/gas/heat meters.

Hexadecimal numbers are marked with a suffix "h". Binary coded numbers are marked with a suffix "b". Numbers without suffix are decimal numbers except another coding is explicitly declared.

## 1.2 Version history

The issue 1.0 is the very first release with the limitation to unidirectional meters only.

The issue 2.0 amends regulation of standard to access a bidirectional meter or actuator. The use of repeaters was substantiated. Parts were adapted to ensure coexistence with NTA 8130.

The issue 3.0 introduces the synchronous transmission timing to support the long term use of a battery powered bidirectional repeater. Some new CI-Fields were adopted to support the consequent use of Short and Long Header for wireless datagrams.

This issue 4.0 extend the applicable security methods. It allows complying with the requirements of the Federal Office for security in information technologies (Bundesamt für Sicherheit in der Informationstechnik - BSI) by applying Annex E. It applies an update according to the new release of the [EN 13757-3:2013] and [EN 13757-4:2013]. Additional two new Layers are introduced, which extend the existing Link Layer and adds a new Layer for authentication and fragmentation of messages. The M-Bus OBIS Reference list is expanded and separated from the OMS M-Bus Data point list.

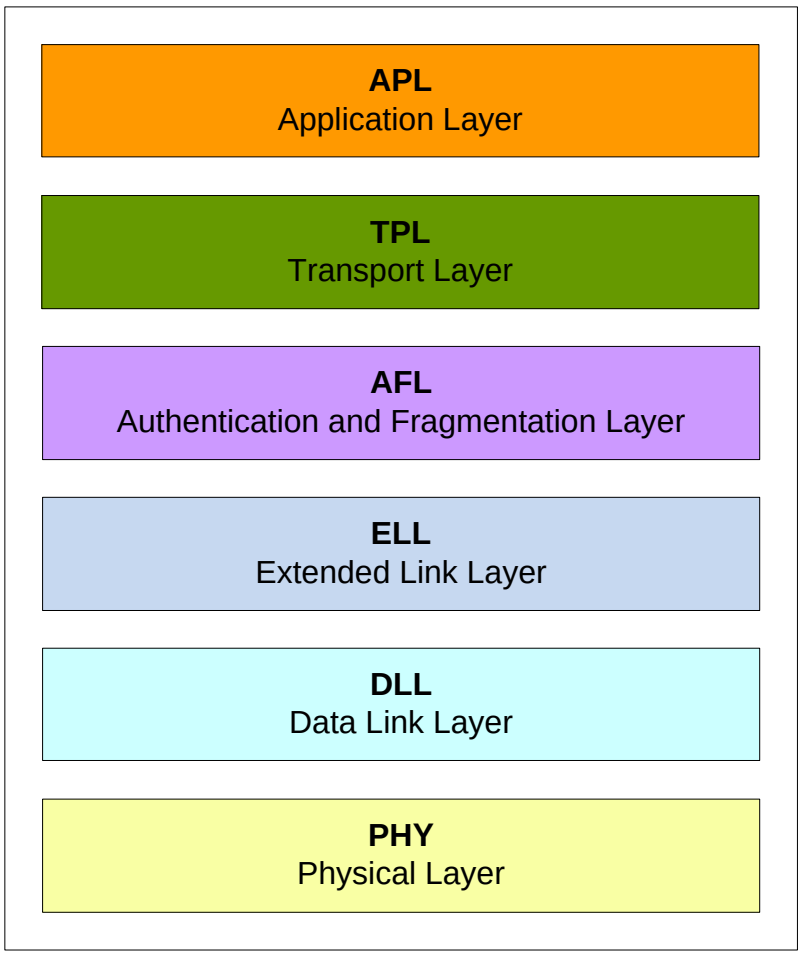
[1] This document shall be applied only together with OMSS Vol.1 Issue 2.0.0 or higher!

# 2 M-Bus Frame Structure

## 2.1 M-Bus-Layer model

The M-Bus Protocol is separated in several layers based on the OSI-communication layer model. This document is structured in the order of applied communication layer presented in Figure 1.

**Figure 1 – M-Bus Layer model**




Physical Layer and Data Link Layer are always present. The Transport Layer and the applied Application Layer (if exist) are always introduced by the CI-Field of the Transport Layer. Optional layers[2] like ELL or AFL are introduced by special CI-Fields. In such case the M-Bus-message contains several CI-Fields, which are chained to one another.

[2] The [EN 13757-5] supports also an additional network layer which is located between ELL and AFL. This layer is never used in the Open Metering System.

## 2.2 Supported CI-Fields

The CI-Field declares the communication layer, the transport direction (not applicable for lower layers like ELL and AFL) and the Application Protocol (if exists). The CI-Field declares also which type of Transport Layer ("None", "Short" and "Long".) is applied.

The following CI-Fields are allowed for OMS-Communication:

**Table 1 – List of supported CI-Fields**

| CI-Field | Function/Layer | Up- or Down-link | Header-Type | Protocol or Service |
|---|---|---|---|---|
| 50h [d] | Application Reset or Select | Down | None | M-Bus |
| 51h [d] | Command | Down | None | M-Bus |
| 52h [d] | Selection of Device | Down | None | M-Bus |
| 53h | Application Reset or Select | Down | Long | M-Bus |
| 5Ah [d] | Command | Down | Short | M-Bus |
| 5Bh | Command | Down | Long | M-Bus |
| 5Fh [a] | Command | Down | Long | Security Management (TLS-Handshake) |
| 60h | Command | Down | Long | DLMS [b] |
| 61h [d] | Command | Down | Short | DLMS [b] |
| 64h [a)] | Command | Down | Long | SML [b] |
| 65h [a, d] | Command | Down | Short | SML [b] |
| 6Ch | Time Sync | Down | Long | Generic |
| 6Dh | Time Sync | Down | Long | Generic |
| 6Eh | Application Error | Up | Short | Generic |
| 6Fh | Application Error | Up | Long | Generic |
| 70h [d] | Application Error | Up | None | Generic |
| 71h [d] | Alarm | Up | None | Generic |
| 72h | Response | Up | Long | M-Bus |
| 74h | Alarm | Up | Short | Generic |
| 75h | Alarm | Up | Long | Generic |
| 7Ah | Response | Up | Short | M-Bus |
| 7Ch | Response | Up | Long | DLMS [b] |
| 7Dh | Response | Up | Short | DLMS [b] |
| 7Eh [a] | Response | Up | Long | SML [b] |
| 7Fh [a] | Response | Up | Short | SML [b] |
| 80h | Pure Transport Layer | Down | Long | None |
| 8Ah | Pure Transport Layer | Up | Short | None |
| 8Bh | Pure Transport Layer | Up | Long | None |
| 8Ch [c] | Extended Link Layer | Up/ Down | Short | Lower Layer Service (2 Byte) |

| | | | | |
|---|---|---|---|---|
| 8Eh [c] | Extended Link Layer | Up/ Down | Long | Lower Layer Service (10 Byte) |
| 90h [a, c] | Authentication and Fragmentation Layer | Up/ Down | variable | Lower Layer Service |
| 9Eh [a] | Response | Up | Short | Security Management (TLS-Handshake) |
| 9Fh [a] | Response | Up | Long | Security Management (TLS-Handshake) |
| B8h [d] | Set baud rate to 300 baud | Down | None | Link Layer Control |
| BBh [d] | Set baud rate to 2400 baud | Down | None | Link Layer Control |
| BDh [d] | Set baud rate to 9600 baud | Down | None | Link Layer Control |
| | | | | |

[a] Planned for a future revision of [EN 13757-3:2013], The released standard mark these CI-Field values as reserved

[b] Refer also [FprEN 13757-1:2012], [EN 62056-6-1:2013], [DLMS UA] or [SML-spec]

[c] These CI-Fields are used for lower layers and may be used in combination with another CI-Field

[d] These CI-Fields shall be used for wired M-Bus only!

## 2.3 Supported Device Types

This specification covers only devices with a Device Type listed in Table 2 or Table 3.

**NOTE:** The Device Types listed in Table 4 may also be integrated in the Open Metering System. However these devices cannot be approved by the OMS-Compliance Test. Therefore the interoperability for these Devices Types cannot be guaranteed.

OMS-Gateways shall accept all the Device Types listed in Table 2 and Table 3. Optionally it may also support Device types of Table 4.

For further details on the Device Types refer to [EN 13757-3:2013], Table 6.

The “category” column gives the mapping from the Device Type to the corresponding OBIS-category / energy type in the “Identification Number for measuring devices applying for all manufacturers” specified in [DIN 43863-5:2012], see chapter 3.2.

**Table 2 – Device Types of OMS-Meter (certifiable with OMS-CT)**

| Device Type | Code | category |
|---|---|---|
| Electricity meter | 02h | 1 |
| Gas meter | 03h | 7 |
| Heat meter | 04h | 6 |
| Warm water meter (30°C ... 90°C) | 06h | 9 |
| Water meter | 07h | 8 |
| Heat Cost Allocator | 08h | 4 |
| Cooling meter (Volume measured at return temperature: outlet) | 0Ah | 5 |
| Cooling meter (Volume measured at flow temperature: inlet) | 0Bh | 5 |
| Heat meter (Volume measured at flow temperature: inlet) | 0Ch | 6 |
| Combined Heat / Cooling meter | 0Dh | 6 |
| Hot water meter (≥ 90°C) | 15h | 9 |
| Cold water meter [a] | 16h | 8 |
| Waste water meter | 28h | F |
| [a] Device Type 16h is to be used for cold drinking water that temporarily has been cooled or heated in order to achieve the wanted temperature (chilling/antifreeze). | | |

**Table 3 – Device Types of other OMS-devices (prepared for OMS-CT)**

| Device Type | Code | category |
|---|---|---|
| Breaker (electricity) | 20h | F |
| Valve (gas or water) | 21h | F |
| Customer unit (display device) | 25h | E |
| Communication controller | 31h | E |
| Unidirectional repeater | 32h | E |
| Bidirectional repeater | 33h | E |
| Radio converter (system side) | 36h | E |
| Radio converter (meter side) | 37h | E |

**Table 4 – Device Types of not certifiable device**

| Device Type | Code | category |
|---|---|---|
| Other | 00h | F |
| Oil meter | 01h | F |
| Steam meter | 05h | F |
| Compressed air | 09h | F |
| Bus / System component | 0Eh | E |
| Unknown Device Type | 0Fh | F |
| Reserved for consumption meter | 10h to 13h | - |
| Calorific value | 14h | F |
| Dual register (hot/cold) water meter | 17h | 9 |
| Pressure meter | 18h | F |
| A/D Converter | 19h | F |
| Smoke detector | 1Ah | F |
| Room sensor (e.g. temperature or humidity) | 1Bh | F |
| Gas detector | 1Ch | F |
| Reserved for sensors | 1Dh to 1Fh | - |
| Reserved for switching devices | 22h to 24h | - |
| Reserved for customer units | 26h to 27h | - |
| Garbage | 29h | F |
| Reserved for Carbon dioxide | 2Ah | F |
| Reserved for environmental meter | 2Bh to 2Fh | - |
| Reserved for system devices | 30h<br>34h to 35h<br>38h to 3Fh | E |
| Reserved | 40h to FEh | - |
| Not applicable (reserved for a wild card search; refer to [EN 13757-3:2013] chapter 11.3 and 11.5.3) | FFh | - |

# 3 Address handling

## 3.1 M-Bus Address

### 3.1.1 Overview M-Bus Address

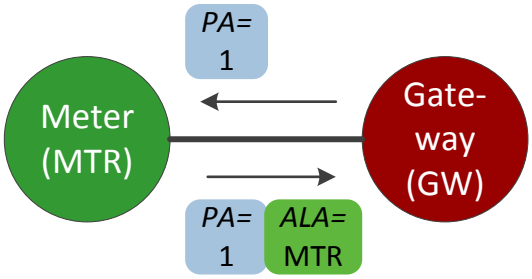
M-Bus defines several types of addressing. The address can be handled in the Data Link Layer (DLL), in the Extended Link Layer (ELL) or in the Transport Layer (TPL). The format of the Address Field (A-Field) is different in each of those layers and even differs between wired and wireless M-Bus. The address used in DLL and ELL is needed for communication establishment whereas the address in the TPL identifies the application itself.

### 3.1.2 Wired M-Bus

#### 3.1.2.1 Primary Address

The A-Field of the wired M-Bus uses a single byte in the DLL which contains always the address of the slave. The address of the master is never used because only one master is allowed on the wired M-Bus. This Link Layer Address is called Primary Address (PA). The unconfigured Primary Address shall be 0. A valid address in the range between 1 and 250 has to be assigned during the configuration process if primary addressing is used. The addresses 251 to 255 are used for special purposes and shall be supported conform to [EN 13757-2:2004].

**Figure 2 – Primary Address for wired M-Bus**




The slave shall always responds with its own valid Primary Address even in the case it is addressed from the master by Secondary Address. Only slaves which do not support a Primary Address shall responses with 253 in this case.

#### 3.1.2.2 Secondary Address

The Secondary Address is an enhancement of the limited address space of the Primary Address. It defines the Application Layer Address (ALA) and shall be worldwide unique for all types of meters. Therefore it shall be assigned by the meter manufacturer and shall not be changeable by the customer or by the user (e.g. MSO).

This rule is not applicable for adapter e. g. pulse adapter, encoder adapter or protocol converter. If an adapter is used to connect the meter with the M-Bus then the Adapter should transmit the Meter address. For this purpose the serial number of the Meter replaces the Identification Number (part of the ALA) of the M-Bus-Adapter. In this case the unchangeable Identification Number of the adapter shall be additionally transmitted in the M-Bus-Data record "Fabrication Number" to avoid unsolvable address collisions.

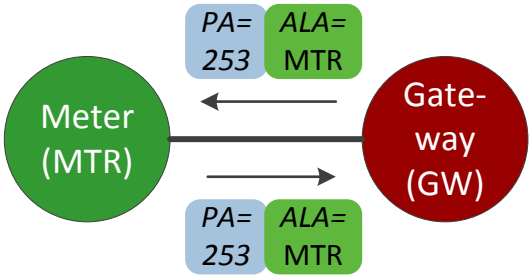
The structure of the Secondary Address is described in chapter 3.1.4. The usage of the Secondary Address is indicated by a Primary Address 253.

The selection of a meter by Secondary Address (refer to [EN 13757-3:2013] chapter 11.3) and the wild card search (refer to [EN 13757-3:2013] chapter 11.5) shall be supported.

An adapter should support the enhanced selection with Fabrication Number (refer to [EN 13757-3:2013] chapter 11.4).

Meters which do not support the enhanced selection shall ignore the enhanced selection command of the master.

**Figure 3 – Secondary Addresses for wired M-Bus**




The ALA of the Meter shall always be in each M-Bus-message of the slave. The master shall apply the ALA of the Meter at least in case of encryption or during the selection (refer to [EN 13757-3:2013]) of the slave (Figure 3).

**NOTE**: The Address field of the ALA exists only if a Transport Layer with Long Header is used (refer to 2.2 and Annex D).

**NOTE**: When a valid Primary Address is applied or the slave is clearly selected then the (unencrypted) message of the master may not contain a Secondary Address (ALA) (Figure 2).

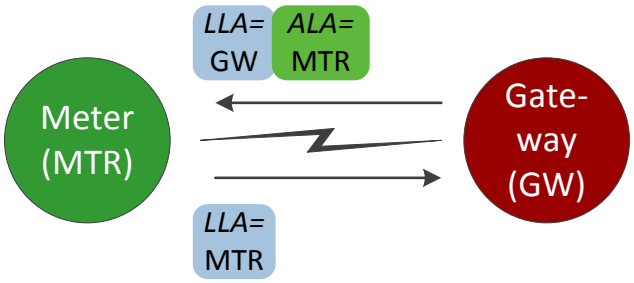
If an adapter uses encrypted data transfer then its Fabrication Number shall be transmitted in the unencrypted area.

## 3.1.3 Wireless M-Bus

### 3.1.3.1 Link Layer Address (LLA)

This Address field of the Data Link Layer always contains the address of the sender. This can be the address of the meter/repeater/gateway (in the case of an integrated radio interface) or the address of the RF-Adapter (which connects the hosted device to the radio channel). The structure is described in chapter 3.1.4. The Link Layer Address shall be used in each wM-Bus-datagram.

**Figure 4 – Addresses for wireless M-Bus (without ELLA)**




For the world-wide uniqueness of the address the Link Layer Address shall be assigned by the manufacturer and shall not be changeable for any other one (like meter side operator). The assignment of an additional address (if necessary e.g. using an external RF-Adapter)

has to be applied in the Transport Layer using an Application Layer Address (refer to chapter 3.1.3.3).

### 3.1.3.2 Extended Link Layer Address (ELLA)

The Address field of the Extended Link Layer always contains the destination address (meter/adapter/gateway). It is only used for wireless M-Bus. The structure is described in chapter 3.1.4.

The ELLA exists only, if a long Extended Link Layer is applied (refer to 5.3).

A received datagram with a wrong ELLA shall be ignored even if the ALA is correct.

The Extended Link Layer Address is only required in the following cases.

*1. Addressing of a not assigned communication partner*

To avoid conflicts in a bidirectional radio communication it is essential, that a meter is allocated to only one dedicated gateway. This allocated gateway should not use the ELLA to contact the Meter (except case 2 or 3 is applicable). Any Other Device (such as a service tool) shall always use the ELLA, to identify themselves as unallocated communication partners on the meter.

*2. Response to a request with ELLA*

If a device receives a datagram with an ELLA (identical to its own Link Layer Address) it shall respond with an ELLA (holding the Link Layer Address of the Other Device). If the received ELLA does not fit to its own Link Layer Address the datagram shall be ignored.

*3. Fragmented Messages*

If a message is fragmented (by using the AFL (refer to chapter 6)) each fragment (datagram) shall apply the ELLA. This is required because the Application Layer Address (ALA) will only be present in the first fragment. Even the request (REQ-UD2) and the acknowledge (ACK) of the concerning fragment shall apply the ELLA of the communication partner (refer also to Annex L).

**NOTE:** The first REQ-UD2 of a fragmented message may contain no ELLA (but always an ALA). The first RSP-UD as well as all following fragments of this message requires the ELLA.

Message types SND-NR, SND-IR, ACC-NR and ACC-DMD should not apply the ELLA.

Figure 5 and Figure 6 shows the usage of the ELLA beside the other address fields.

**Figure 5 – Addresses for wireless M-Bus (with ELLA)**

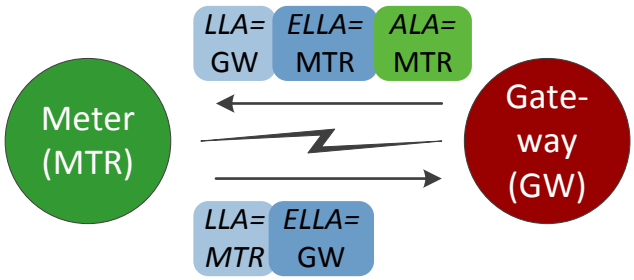
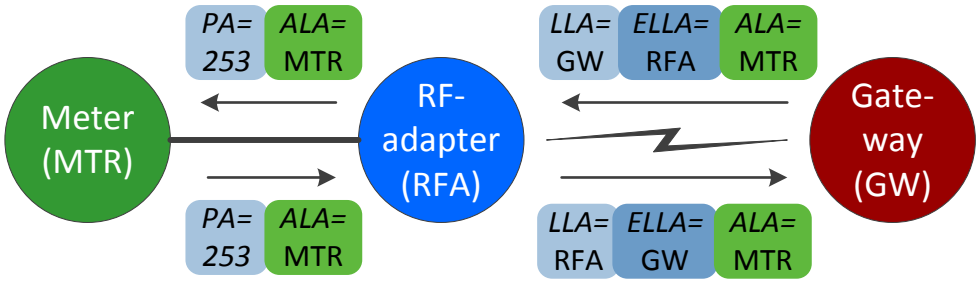


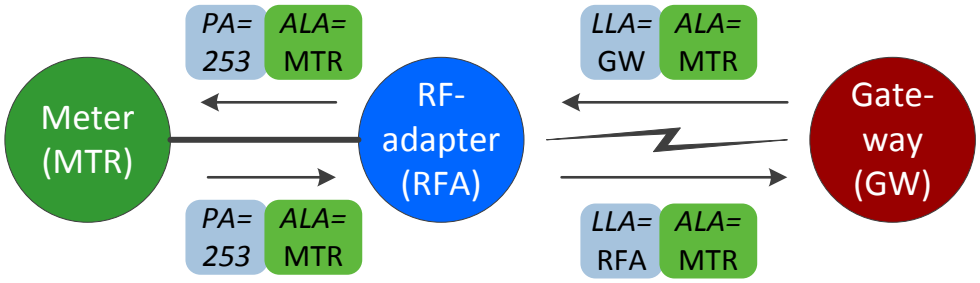
**Figure 6 – Addresses for wired and wireless M-Bus (with ELLA)**




### 3.1.3.3 Application Layer Address (ALA)

The address field of the Transport Layer contains always the address of the application (Meter/Actuator). The structure is described in chapter 3.1.4.

**Figure 7 – Addresses for wired and wireless M-Bus (without ELLA)**




The Application Layer Address shall always be present in downlink messages (to the meter) and in uplink messages (from the meter) if an external RF-Adapter (Device Type 37h) is used (refer to Figure 7). For Meters/Actuators with an integrated radio module the Link Layer Address acts as Application Layer Address as well.

A received datagram with a wrong ALA (if exists) shall be ignored by the meter even if the ELLA is correct.

**NOTE**: In case of service the RF-Adapter can also be direct addressed using the ALA with the RF-Adapter address.

**NOTE**: The address of the gateway or communication partner is never applied in this address field.

**NOTE**: The Address field of the ALA exists only if a Transport Layer with long header is used (refer to 2.2 and Annex D).

**NOTE**: The additional usage of an ALA is also allowed (but not requested) when LLA and ALA are identical.

## 3.1.4 M-Bus Address elements

The LLA and ELLA for wireless M-Bus as well as the ALA (for both wired and wireless M-Bus) always consist of these four parts:

- Identification Number (Device ID)
- Manufacturer ID
- Version
- Device Type

The usage of these elements shall conform to [EN 13757-3:2013] chapter 5.5 to 5.8.

The Manufacturer ID shall be registered at the Flag association (http://www.dlms.com/organization/flagmanufacturesids/index.html).

Note that the Version Field is not restricted in use as software version. It may apply also for other address purposes like coding of the manufacturer's location as long as it grants a worldwide unique addressing of this meter. Additional meter identification schemes like customer number or meter location may be implemented via corresponding data records within the Application Layer.

Refer to chapter 2.3 for the limitation of the Device Type.

The order of the address elements differs between LLA, ELLA and the ALA.

The ALA shall apply an order given in [EN 13757-3:2013] chapter 5.4.

The LLA and ELLA shall apply an order given in [EN 13757-4:2013] chapter 5.13.

An address example can be found in Annex C of [EN 13757-3:2013] and Annex N of this specification.

## 3.2 DIN Address according to the DIN 43863-5

The [DIN 43863-5:2012] defines a common structure Meter-ID. This DIN-Address structure is the base for the meter management.

The structure of the DIN-Address is presented in Table 5.

**Table 5 – Structure of the DIN-Address**

| **Digit** | 14 | 13 | 12 | 11 | 10 | 09 | 08 | 07 | 06 | 05 | 04 | 03 | 02 | 01 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Meaning** | OBIS-cat.[3] | Manufacturer ID | | | Fabrication Block | | Fabrication Number | | | | | | | |
| **Example** | 7 | Q | D | S | 0 | 1 | 1 | 1 | 2 | 2 | 3 | 3 | 4 | 4 |

The DIN Address may be used on the label of a Metering Device. For the Link or Transport Layer of the wired or wireless M-Bus only the M-Bus Address is allowed. However there is a clear relation between the M-Bus Address and the DIN Address and one address type can be converted to the other one. The address conversion shall be done according to following rules.

OBIS-cat.[3] — Energy type (e.g. electricity) based on OBIS code value group A. (Note that categories “E” and “F” are listed in DIN 43863-5:2012, but only energy type “F” for “Other media” is listed in Blue Book ed. 11 of DLMS User Association.)
For the conversion between the address types use Table 2; Table 3 and Table 4 in 2.3. These tables list the assigned OBIS- category / energy type for each M-Bus Device Type.

Manufacturer ID — This field corresponds to the Manufacturer ID of the M-Bus Address. Note that Manufacturer ID of the DIN Address is presented with ASCII-letters (A-Z, upper case only), whereas M-Bus is using a 2 byte binary code. The conversion between both is described in [EN 13757-3:2013] chapter 5.6. The most significant bit of the M-Bus Manufacturer ID is pre-set to 0 (Hard address).

Fabrication Block — According to [DIN 43863-5:2012] the usage of the Fabrication Block is manufacturer specific. This is comparable with the Version Field of the M-Bus Address. For the conversion between M-Bus Address and the DIN-Address the Fabrication Block gets the same content like the Version Field (and vice versa).

[3] Corresponds to “OBIS- category / energy type”

| | |
|---|---|
| Fabrication Number | The Fabrication Number contains the serial number of the meter. It is equal to the Identification Number of the M-Bus Address. For the conversion between address types the Fabrication Number of the DIN-Address gets the same content like the Identification Number of the M-Bus Address (and vice versa). |

Each M-Bus Device Type can be unambiguously converted to an OBIS-Category. Since conversely, multiple Device Types are mapped to a single OBIS- category / energy type, a conversion can be unique only if all Device Types with the same OBIS- category / energy type differ in Identification Number, Manufacturer ID or Version. Thus, the manufacturer shall ensure that the M-Bus Addresses of all of their meters have unique combinations of Identification Number and Version within the same OBIS- category / energy type.

# 4 Physical Layer

Data shall be collected from the meters using two-wire M-Bus via pull mode, or encrypted wireless M-Bus (wM-Bus) via push mode. This means that the meters transmit metering data by RF in regular intervals or they have to be queried via wired M-Bus by the gateway. Optionally the gateway may also query metering data from bidirectional wireless M-Bus Meters.

## 4.1 Twisted Pair Connection (M-Bus)

### 4.1.1 Electrical Specification

For wired connections the Physical Layer M-Bus according to the European standard [EN 13757-2:2004] is used. It is a two-wire system which optionally also provides power to the devices. The number of M-Bus devices which can be controlled by a gateway shall be specified by the manufacturer. The minimum requirements are those of a Mini-Master as described in [EN 13757-2:2004]. In addition the gateway shall fulfil the requirements of Annex C.

### 4.1.2 Hardware Connections and Cable

The bus interfaces of the slaves are polarity independent, which means the two bus lines can be interchanged without affecting the operation of the slaves. Besides protection aspects, this also results in a simplified installation of the bus system. In order to maintain correct operation of the bus in case of a short circuit of one of the slaves, these must have a protection resistor with a nominal value of 430±10 Ω in their bus lines. This limits the current in case of a short circuit to a maximum of 100 mA (42 V / 420 Ω), and reduces the energy converted into heat in the bus interface. For the requirements for wiring and installation refer to [EN 13757-2:2004]

## 4.2 Wireless Communication (wM-Bus)

### 4.2.1 Modes and Requirements

The [EN 13757-4:2013] describes various variants for wireless meter communication. They cover all types of meter communication including mobile and stationary readout modes. The Open Metering System scenario requires a stationary receiver and frequent transmission of meter data to support consumer consumption feedback and variable tariffs. The extension to [EN 13757-4:2013] by this document allows optional single hop relaying to extend the radio range. Multi hop relaying of these data via other (optionally battery powered) meters is not supported by this specification. Note that the [EN 13757-5] covering such relaying via meters does not apply to the proposed modes S,T and C.

As for the various modes described in [EN 13757-4:2013], only the modes S1, S2, T1, T2, C1 and C2 are supported by this specification. These modes operate in duty-cycle limited sub bands of the 868 – 870 MHz license free frequency range. The duty cycle does not limit the functions required for the Open Metering System but limits the band occupation time from other systems operating in these frequency bands.

The newly introduced modes C1 and C2 provide a more efficient NRZ channel coding which is widely supported by modern RF chips.

Note, a limitation of the total average transmission duty cycle per hour to 0.02 % is recommended for all radio communication modes. This is required to limit the collision rate in

dense or repeated situations. The CEPT/ERC/REC 70-03 E, see [ERC 70-03], and the ETSI EN 300220-1 [ETSI-ERM] standards describes further requirements for the Physical Layer.

S1, T1 and C1 are unidirectional modes where the meter frequently (seconds to hours) transmits datagrams containing meter identification together with metered data. This unidirectional function is sufficient to support all required communication functions for a basic meter within the framework of the Open Metering System.

S2, T2 and C2 are compatible bidirectional enhancements of the respective unidirectional modes. They enable an optional gateway to meter communication after a meter to gateway datagram. The [EN 13757-4:2013] describes all requirements (also applicable for testing conditions) for the supported modes S1, S2, T1, T2, C1 and C2. For the S2 mode only the variant with long preamble is supported.

Due to required battery lifetime, most meters and some actuators cannot support a continuous receive mode. A gateway initiated ("Pull") communication with the meter or actuator is possible, but any such (downstream) communication is typically limited to a time slot directly after an upstream communication (except for mains powered devices). Since the meter transmits frequently, the resulting possible transmission delay (of seconds to hours) seems acceptable. An actuator shall transmit at least its unique ID and its status and wait after each transmission for a possible datagram from the gateway as described in [EN 13757-4:2013]. For a breaker, as the typical actuator, the maximum time interval between such transmissions shall be the same as the maximum time interval for meter transmissions of the same medium (i.e. electricity or others) as shown in Table 7.

For certain communication between the gateway and an optional actuator this might not be sufficient. Thus, actuators with faster reaction time requirements should be mains powered.

The Link Control Bits in the Extended Link Layer or Configuration Field of the meter datagram signals to the gateway whether the device can receive data (i.e. implements the bidirectional modes), and whether it can receive continuously or only directly after each transmission.

The meter and gateway manufacturers decide which of the supported modes are implemented in their products. This requires clear labelling of both, the meter and the gateway as well as the corresponding data sheets so that the customer can choose between interoperable combinations. Note that a gateway may support the communication with one, several or with all of the mentioned radio communication modes.

Note also that the Link Layer itself does not support multi-datagram messages. Functions requiring more data than the maximum length of a datagram shall handle a fragmentation of long messages via the Authentication and Fragmentation Layer (refer to chapter 6).

Countries being members of CEPT (e.g. EU, EEA and more) shall use the frequencies specified in [EN 13757-4:2013], which are based on CEPT/ERC/REC 70-03 [ERC 70-03] (except Russia). Other countries where these frequencies are not allowed shall use the alternative frequencies defined in Annex O to the OMSS Non-European Frequencies [OMS-NEF].

### 4.2.2 Wireless Data Transmission Intervals

Depending on the application there are different requirements for the maximum update period. For a typical 95 % probability of a reception in spite of possible collisions, each datagram has to be transmitted at least twice within this maximum update period. Note that according to CEPT/ERC/REC 70-03 E [ERC 70-03] there should be a minimum time delay between successive transmissions. Table 6 shows this off time advised by [ERC 70-03] for the supported modes.

**Table 6 – Minimum transmitter "off" time in seconds**

| | Mode S | Mode T | Mode C |
|---|---|---|---|
| Meter to Other Device | 1.8 s | 0.72 s | 0.72 s |
| Other Device to Meter (bidirectional communication) | 1.8 s | 1.8 s | 3.6 s |

Therefore a bidirectional meter/actuator shall apply a response delay according to [EN 13757-4:2013] for every datagram which responses to a request or command of the communication partner.

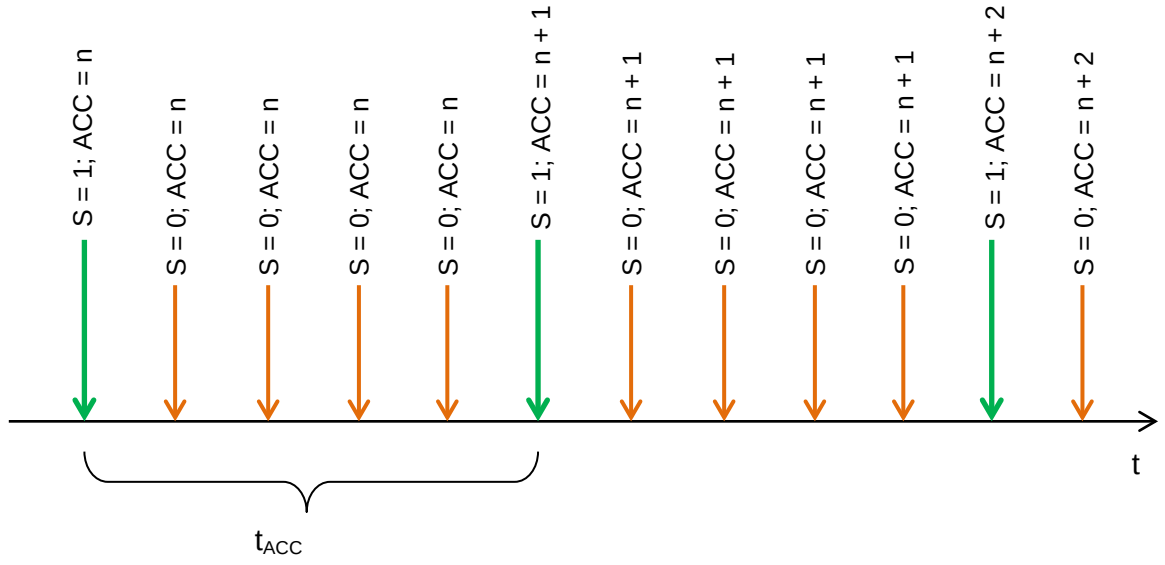
### 4.2.2.1 Synchronous versus asynchronous transmission

OMS meters shall use the strictly synchronous transmission scheme specified in [EN 13757-4:2013], chapter 11.6.2.

If the Extended Link Layer is present, the Access Number and Synchronous Bit (refer to 5.3.3) in the ELL shall be used for the synchronous timing. Otherwise the Access Number of the Transport Layer and the Synchronous Bit in the Configuration Field shall be applied.

As described in [EN 13757-4:2013], chapter 11.6.2, additional asynchronous transmissions are allowed. The Access Number handling of asynchronous transmissions is specified in [EN 13757-3:2013], chapter 5.9.2 and pictured in Figure 8.

**Figure 8 – Access number for synchronous and asynchronous transmissions**




*Legend:*

| | |
|---|---|
| S | S = 1: synchronous datagram; S = 0: asynchronous datagram |
| ACC | Access Number |
| $t_{ACC}$ | individual transmission interval from the datagram with the Access Number ACC=n to the next synchronous transmission with ACC=n+1 |

The synchronous transmission shall be one of the message types SND-NR, ACC-DMD or ACC-NR (refer to Table 11). If the nominal transmission interval (refer to [EN 13757-4:2013] chapter 3.1.8 and 11.6.2) is smaller than the selected update interval of consumption data (refer to Table 7) then one or several ACC-NR may be used for synchronous transmission between the synchronous transmissions of the SND-NR. The ratio of ACC-NR versus SND-NR (respectively ACC-DMD in case of alert) shall be n/1 to allow a reception of every $n^{th}$ datagram only (with n = 0 … 15) by a battery operated receiver. The ratio shall not be changed after the installation of the meter/actuator.

The start of the first synchronous transmission shall be stochastic. It is not allowed to fix the synchronous transmission exactly to a common event like a special time or a power on after a central voltage drop. This is required to avoid a concurrent use of the radio channel by many meters. Refer also to chapter 7.2.2.1.

### 4.2.2.2 Interval of consumption data

An update of consumption data with every synchronous transmission is recommended. However the consumption data shall be updated at least with the average update interval maximum as listed in Table 7 plus additional scatter.

See the following table for the mandatory data update periods:

**Table 7 – Update interval of consumption data for different media**

| **Metering media** | **Mandatory (billing and actuator)** | | **Informative aspects (consumer)** |
|---|---|---|---|
| | Average update interval maximum [min] | Visualization interval for energy provider [hour] | Visualization interval for consumer [min] |
| Electricity | 7.5 | 1 | 15 |
| Gas | 30.0 | 1 | 60 |
| Heat (district heating) | 30.0 | 1 | 60 |
| Water / Warm water | 240.0 | 24 | – |
| Heat cost allocators | 240.0 | 24 | – |
| Heat / Cold (sub metering) | 240.0 | 24 | – |
| Repeater[4] | 240.0 | – | – |

Table 7 shows data visualization intervals for informative and billing aspects. For consumers, the visualization intervals for different media are 15 respectively 60 minutes at a typical reception probability of more than 95 %. Informative intervals are given to provide current data for consumers.

### 4.2.2.3 Interval of installation data

The optional transmission of installation datagrams (with C = 46h) should happen only after a manual installation start event (e.g. push installation button). Installation datagrams shall be transmitted at least 6 times with an interval of 30 to 60 seconds. The transmission of installation datagrams shall stop no later than 60 minutes after the manual start event. Note that the duty cycle shall be observed also during installation mode. If the installation datagram contains fixed data for meter management (like OBIS code definitions, as defined in [EN 13757-3:2013] Annex O.2), it shall be marked as a static message (refer to Table 24).

### 4.2.2.4 Interval of management data

If the meter/actuator provides special management data (static data only, no consumption data or other time variant data) then it shall mark this as a static message (refer to Table 24) and send it at least twice a day.

[4] Limit refers to datagrams which are generated by the repeater itself. Not for repeated datagrams!

## 4.2.3 Access Timing of a bidirectional Meter or Actuator

### 4.2.3.1 Detection of the accessibility

A meter/actuator signals its own accessibility in the Link Control Bits of every transmission. These bits are located in either the Extended Link Layer (see 5.3.3) or the Configuration Field (Encryption Mode 0 and 5 only) (refer to see 7.2.4.6). The meter/actuator initiates periodical transmissions. If the gateway wants to transmit a message to a meter it checks the Link Control Bits if the meter is accessible.

**Table 8 – Accessibility of a meter/actuator**

| Bit B | Bit A | Accessibility of a meter/actuator |
|---|---|---|
| 0 | 0 | Meter/actuator provides no access windows (unidirectional meter) |
| 0 | 1 | Meter/actuator supports bidirectional access in general, but there is no access window after this transmission (e.g. temporarily no access in order to keep duty cycle limits or to limit energy consumption) |
| 1 | 0 | Meter/actuator provides a short access windows only immediately after this transmission (e.g. battery operated meter) |
| 1 | 1 | Meter/actuator provides unlimited access at least until the next transmission (e.g. mains powered devices) |

Unidirectional meters (modes S1, T1 or C1) are never accessible. Unidirectional actuators are not allowed.

Mains powered meters or actuators may provide an unlimited access, and the gateway may send a command or a request at any time.

Battery operated bidirectional devices are very restricted in their power consumption. Typically they will provide a short access window only immediately after a transmission. The gateway or other communication device (as master) may initiate a communication to the meter/actuator (as a slave) during this timeslot. The timing conforms to [EN 13757-4:2013] and depends on the mode. The [EN 13757-4:2013] defines for S2 and T2-mode a response time $t_{RO}$ after a transmission. For the C2-mode a response delay $t_{RO\_slow}$ shall always be applied.

The response time $t_{RO}$ respectively $t_{RO\_slow}$ shall be calculated from the end of the post-amble of meter transmission to the start of the gateway transmission. The transmission of the first chip (bit) of the preamble shall start before the maximum delay of $t_{RO}$ respectively $t_{RO\_slow}$ expires, and the meter shall then receive the transmission from the gateway or another device correctly.

**Figure 9 – Access timing of a meter/actuator with short access windows (T-Mode example)**

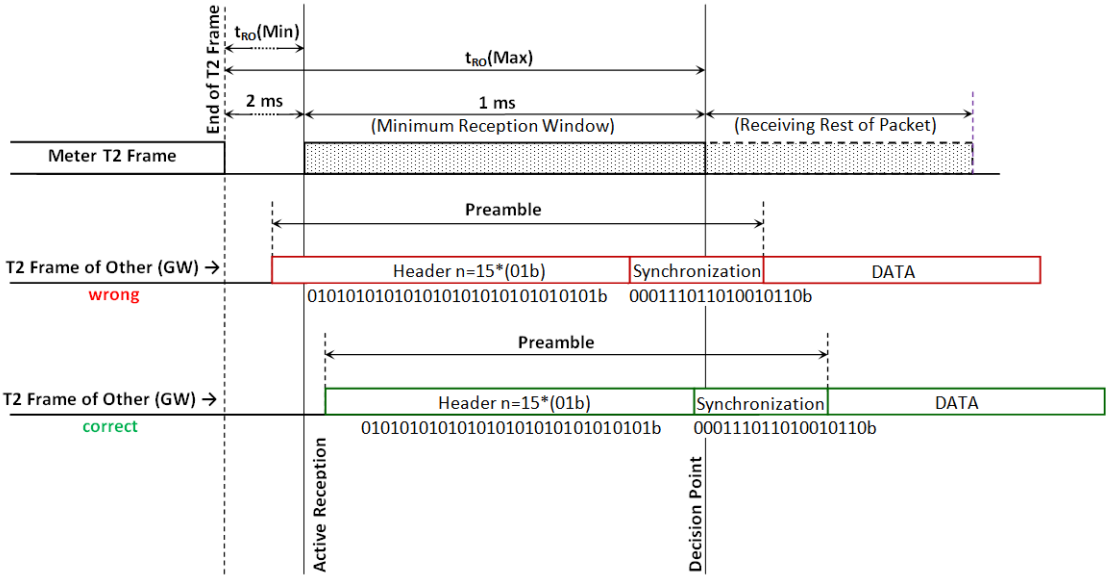



Figure 9 shows both correct and wrong access timing to a meter device. The minimum of preamble length according to [EN 13757-4:2013] shall be inside the minimum reception windows of the receiver. However if the preamble uses more than the minimum preamble length it may start earlier, accordingly.

### 4.2.3.2 Preamble length

The modes S1, S2, T1 and T2 in [EN 13757-4:2013] have no limits of the maximum preamble length. This allows a Denial of Service-Attack to a battery operated meter, actuator or repeater. To prevent this, the transmitted preamble length according to this OMS-Specification shall be within the limits of Table 9.

**Table 9 – Limits of transmitted preamble length**

| Mode and submodes | Preamble length [b] | | Unit |
|---|---|---|---|
| | Min. | Max. | |
| S1 | 576 | 592 | Chips |
| S2 [a] | 576 | 592 | Chips |
| T1 | 48 | 64 | Chips |
| T2 [a, c] | 48 | 64 | Chips |
| C1 | 64 | 64 | Chips |
| C2 [a] | 64 | 64 | Chips |

[a] Up- and downlink
[b] Number of chips including synch. pattern
[c] Note, the preamble differs between uplink and downlink

**NOTE**: Since the [EN 13757-4:2013] allows even longer preambles a receiver may support also a longer preamble length (as given in table above), as long as its energy budget permits.

#### 4.2.3.3 Frequent Access Cycle

Bidirectional meters/actuators shall support the Frequent Access Cycle as defined in [EN 13757-4:2013] chapter 11.6.3.3.

### 4.2.4 Transmissions Limits and Transmission Credits

A meter/actuator has a nominal transmission interval (refer to [EN 13757-4:2013] chapter 3.1.8 and 11.6.2). This results in a nominal number of transmissions (transmitted datagrams) each day. Bidirectional devices offer the possibility to request/ send additional transmissions from/to the meter/actuator. The number of additional transmissions is controlled by the gateway.

Battery powered devices are limited in their power consumption. Mains and battery powered devices are limited by the duty cycle. Therefore it may happen that the meter/actuator has to stop communication if the gateway or another communication unit sends to many commands or requests.

To handle this state every bidirectional meter/actuator needs an internal register of transmission credits for counting each additional transmission. The generation of a transmission credit is a periodical event. The interval depends on the number of transmission credits per day. A bidirectional meter shall generate at least 6 transmission credits per day. Hence a transmission credit shall be generated at least every 4 hours. However it is recommended that number of credits generated for bidirectional communication is 5 % or higher compared to the number of unidirectional transmissions. Unused credits shall be cumulated for at least 30 days.

When all transmission credits are used up (0 credits left) the meter shall mark this state by the bits B=0; A=1 (refer to Table 8) of the last responded datagram and every following spontaneous transmitted datagram until a sufficient number of transmission credits are obtained. During this period a gateway has no access to the meter/actuator. If more than 3 transmission credits are available again, the meter/actuator should mark this accessibility by the bits B=1; A=0 or B=1; A=1 (refer to Table 8) in the next transmissions. The meter/actuator shall provide at least 1 transmission with an enabled access windows (B=1) within next 12 hours after the first transmission without access (B=0; A=1).

## 4.3 Power Line Communication

Power line communication (PLC) for the primary communication is stipulated as a future option.

# 5 Data Link Layer

## 5.1 Wired Communication (M-Bus)

The Link Layer is fully described in [EN 13757-2:2004]. The requirements to the addressing of wired M-Bus devices are described in chapter 3.1.2. Requirements to the M-Bus-master are listed in Annex C.

The Annex N of this specification contains examples of M-Bus-datagrams.

## 5.2 Wireless Communication (wM-Bus)

The Data Link Layer has always a fix length of 10 bytes (without CRC). There after follows a CI-Field introducing structure and length of the next layer. Such next layer can be the Extended Link Layer (refer to chapter 5.3), the Authentication and Fragmentation Layer, a pure Transport Layer (without Application protocol) or the combined Transport/Application Layer.

The Data Link Layer with Frame Format A as described in [EN 13757-4:2013] shall be used for wireless communication. Link Layer encryption shall not be applied. The requirements to the addressing of wireless M-Bus devices are described in chapter 3.1.3.

The Annex C of the [EN 13757-4:2013] contains datagram examples from the application data down to a bit stream. See also to Annex N of this specification for examples of different message types.

### 5.2.1 Supported C-Fields

The C-Field is used to declare the message types. It is conform to the unbalanced C-Fields of [EN 60870-5-2].

There are different message types for data exchange:

- Spontaneous messages without reply
- Commands from master to slave with acknowledge
- Data requests with response from slave to master
- Commands from master to slave with a immediately response
- Special messages for installation or alarm

The message type is signalled by the C-Field.

The following C-Fields may be generated by the master (gateway or other communication device) and shall be accepted by the slave (meter/actuator).

**Table 10 – C-Fields of master (gateway or other communication device)**

| Message types of master | C-Fields (hex) | Explanation | Required response of bidirectional slave |
|---|---|---|---|
| SND-NKE | 40h | Link reset after communication;<br>Also signals capability of reception of a meter/ actuator after reception of installation datagrams | - |
| SND-UD2 [b] | 43h | Send command with subsequent response (Send User Data 2) | RSP-UD |
| SND-UD [a] | 53h, 73h | Send command (Send User Data) | ACK |
| REQ-UD1 [a] | 5Ah, 7Ah | Alarm request , (Request User Data Class1) | ACK, RSP-UD |
| REQ-UD2 [a] | 5Bh, 7Bh | Data request (Request User Data Class2) | RSP-UD |
| ACK | 00h | Acknowledge the reception of the ACC-DMD | - |
| CNF-IR | 06h | Confirms the successful registration (installation) of meter/actuator into this gateway | - |
| [a] The use of bits FCB, FCV shall conform to [EN 60870-5-2]<br>[b] The SND-UD2 shall be used in wireless M-Bus only and not for fragmented messages | | | |

Only the message type SND-UD and SND-UD2 can be applied to transport application data to a meter/actuator.

The meter/actuator may send spontaneously or as a reaction to a gateway-datagram the following message types:

**Table 11 – C-Fields of slave (meter or actuator)**

| Message types of slaves | C-Fields (hex) | Explanation | Required response of master |
|---|---|---|---|
| SND-NR [b] | 44h | Send spontaneous/periodical application data without request (Send /No Reply) | - |
| SND-IR | 46h | Send manually initiated installation data<br>(Send Installation Request) | CNF-IR |
| ACC-NR | 47h | Contains no data – signals an empty transmission or provides the opportunity to access the bidirectional meter, between two application data transmissions. | - |
| ACC-DMD | 48h | Access demand to master in order to request new important application data (alerts) | ACK |
| ACK [a] | 00h, 10h, 20h, 30h | Acknowledge the reception of a SND-UD (acknowledgement of transmission only);<br>It shall also be used as a response to an REQ-UD1, when no alert happened | - |
| RSP-UD [a] | 08h, 18h, 28h, 38h | Response of application data after a request from master (response of user data) | - |
| [a] The use of bits ACD and DFC shall conform to [EN 60870-5-2]<br>[b] The SND-NR shall be used in wireless M-Bus only and not for fragmented messages | | | |

Only message types RSP-UD and SND-NR can be applied to transport application data from a meter/actuator to the gateway. SND-IR should be applied to transport application data for installation and management purposes only. If a meter or an actuator does not support alarm

functions it shall acknowledge a REQ-UD1 with an ACK. Otherwise it should react according to [EN 13757-3:2013] Annex D.

Uni- and bidirectional Meters/actuators shall support message type SND-NR. Optionally SND-IR (for support of tool-less installation mode for gateways without external installation support) and ACC-NR (see 4.2.2.1) may be supported by the basic meter.
The slave shall reply to every datagram of the master with an expected response, according to

Table 10 independently of whether this datagram was already received earlier (refer to chapter 7.2.2). Exceptions to this rule are described in chapter 4.2.3. The timing and interaction between different message types are shown in Annex L.

## 5.2.2 Optional Repeater for the Wireless Communication

If a direct wireless transmission between a meter/actuator and a gateway is not possible a single intermediate repeater might be used. Such a repeater shall be able to work without complex installation procedures and without routing capability. For a common device management a repeater shall send datagrams with its own address to provide device management data like status. A repeater conforms to general rules like every meter/actuator. The repeater has to send this data periodically (refer to Table 7). It may optionally send installation datagrams (with C = 46h) within given time limits (refer to chapter 4.2.2).

A repeater may be a dedicated device or a function integrated into a meter or a gateway. An integrated repeater should use the address of the hosted meter or the gateway. Both integrated and dedicated repeaters should always apply the Device Type “unidirectional repeater” or “bidirectional repeater” (refer to Table 3) for the transmission of repeater management data.

It will be distinguished between:

- Unidirectional repeaters (repeat datagrams from the meter upward to the gateway only)
- Bidirectional repeaters (repeat datagrams in both directions; from the meter/actuator upwards to the gateway, and from the gateway downwards to the addressed meter/actuator)

### 5.2.2.1 Unidirectional Repeater

The unidirectional repeater repeats only datagrams with C-Fields C = 46h or C = 44h. All other datagrams shall be ignored.

It just retransmits (with some delay) a received Open Metering System compatible datagram when the Hop Counter Bit = 0 and Repeated Access Bit = 0 only. The Hop Counter Bit (bit H) and Repeated Access Bit (bit R) are placed either in the CC-Field of the Extended Link-Layer (see chapter 5.3.3 and 5.3.4) or in the Configuration Field in the Transport Layer (see chapter 7.2.4.3). The repeater shall increment the Hop Counter Bit to 1 before the retransmission, what requires the recalculation of the CRC value for the second block. Datagrams which not provide a Hop Counter Bit shall be ignored.

**NOTE:** The R-Bit was in previous versions declared as the upper bit of the Hop Counter.

The retransmission should be randomly delayed for at least 5 seconds and no more than 25 seconds after reception time. Due to this delay it is not possible to calculate accurately the actual consumption (power, flow) based on the difference of the index values of subsequent datagrams. Also the transfer of the meter time will not be accurate.

**NOTE:** It is intended to provide in the future a description of methods and functionality of a bidirectional repeater without these limitations.

If the repeater receives an installation datagram (with C = 46h) with a Hop Counter = 0 it shall additional generate a SND-NKE message to confirm the ability of receiving this meter to an optional installation service tool. This message shall be generated with a reaction delay of between 2 and 5 seconds after retransmission of the meter message. The installation procedure with repeater is shown in Annex L.

Note that the repeater itself is responsible for staying within duty cycle limits and off time limits in any case.

#### 5.2.2.2 Bidirectional Repeater

A fully functional bidirectional repeater will be defined in a separate volume of the OMS specification.

### 5.2.3 Rules for the gateway

If the gateway receives an installation datagram with C = 46h and with a Hop Counter = 0 it shall generate an SND-NKE to confirm the ability to receive this meter to an optional installation service tool. This message shall be generated within a random delay between min. 5 and max. 25 seconds after the direct reception of a meter installation datagram. In addition it may generate a CNF-IR message to the meter to signal its assignment to this gateway.

In case of an erroneous multiple assignment of one meter/actuator to several gateways, collisions may happen when more than one gateway accesses a meter/actuator. To solve this failure every gateway shall support a collision avoidance mechanism as defined in Annex I. This mechanism describes a random access taking effect after the second unsuccessful access attempt to a meter or an actuator.

The gateway shall provide a clock synchronisation service (refer to chapter 8.5).

# 5.3 Extended Link Layer

## 5.3.1 General

The Extended Link Layer (ELL) is defined in [EN 13757-4:2013] as an extension of the regular Link Layer. The Extended Link Layer shall be applied for wireless M-Bus only.

## 5.3.2 Structure of the Extended Link Layer (ELL)

There is a short and long Extended Link Layer. The long ELL provides an additional address field, which contains always the address of the receiver. This Extended Link Layer Address (ELLA) is structured in same way like the Link Layer Address of Radio datagrams (refer to [EN 13757-3:2013] chapter 5.13)

**NOTE**: The [EN 13757-4:2013] supports additional types of Extended Link Layers which are not supported by the OMS.

**Figure 10 – Short ELL without receiver address**

| | | |
|---|---|---|
| CI = 8Ch | CC | ACC |

**Figure 11 – Long ELL with receiver address**

| | | | | | | |
|---|---|---|---|---|---|---|
| CI = 8Eh | CC | ACC | Manuf. | Ident. no | Ver. | Dev. |

*Legend:*

| | |
|---|---|
| CC | Communication Control Field (refer to 5.3.3) |
| ACC | Access number (refer to 7.2.2) |
| Ident. No | Identification Number (serial number) (part of receiver address) |
| Manuf. | Manufacturer Acronym (part of receiver address) |
| Ver. | Version (part of receiver address) |
| Dev. | Device Type (part of receiver address) |

## 5.3.3 The Communication Control Field (CC)

The Communication control field uses a structure as shown in Table 12

**Table 12 – Definition of the Communication Control Filed (CC)**

| MS Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | LS Bit 0 |
|---|---|---|---|---|---|---|---|
| Bidirectional communication | Delay (always 0) | Synchronous | Hop Counter | Priority (always 0) | Accessibility | Repeated Access | Reserved (always 0) |
| B | 0 | S | H | 0 | A | R | 0 |

The link control bits B, A, S, R, H are also in the Configuration Field present if Encryption Mode 0 or 5 is selected (see chapter 7.2.4.2 and 7.2.4.3). For the case that both the CC-Field and the Configuration Field in the datagram exist, only the link control bits of the CC-Field shall be applied and the link control bits of the Configuration Field shall be ignored.

The bit S shall be used as described in chapter 4.2.2.1.

The bits B and A shall be used as described in chapter 4.2.3.1.

The bit H is used as a Hop Counter to indicate a repeated transmission. The meter, actuator or gateway shall transmit bit H always with zero. The bit R is reserved for use in repeated messages. The meter or actuator shall transmit bit R always with zero. A meter/actuator may ignore a received bit R.

### 5.3.4 Condition to apply the Extended Link Layer

The Extended Link Layer shall always be applied for all kind of message types. There is one exception due to downward compatibility to former OMS specifications. A unidirectional device (meter or adapter) which only uses encryption mode 5 (and 0) can omit the ELL for all applicable message types (SND-NR; SND-IR or ACC-NR). A mixture of using and not using the ELL is not allowed.

**NOTE:** Without using the ELL it is not possible to transmit new data with asynchronous transmissions (see 7.2.2.1).

**NOTE:** The usage of the ELL may also applicable for Encryption Mode 5 in the case of a meter with internal encryption function and an external RF-Adapter. Both functions, the Encryption Mode 5 and the generation of synchronous transmissions, use and increment the Access number. For that reason two Access Numbers are necessary.

Typically the usage of the short ELL is sufficient. Special cases which require the long ELL are described in chapter 3.1.3.2.

# 6 Authentication and Fragmentation Layer

## 6.1 Introduction

This section explains the usage of the Authentication and Fragmentation Layer (AFL) in combination with the other layers and Encryption Modes used in OMS.

The Authentication and Fragmentation Layer provides three essential services:

- Fragmentation of long messages in multiple datagrams
- A Message Authentication Code (MAC) to prove the authenticity of the TPL and APL
- A Message Counter that is required for the Key Derivation Function (refer to chapter 9.4)

This optional layer shall be applied if at least one of these services is required.

Fragmentation is required to transport large messages, like Software update or certificates for the TLS-handshakes (see Annex F). The AFL is separated in a section for each single fragment and a section for the whole message. The position of the AFL in the M-Bus Layer Model is shown in Figure 1.

The MAC (see chapter 9.3.1) protects all layers above the AFL. Therefore no changes in higher layers are possible, as soon as the MAC has been calculated.

## 6.2 Structure of the AFL

### 6.2.1 Overview

**Figure 12 – All Authentication and Fragmentation Layer (AFL) fields**

| CI | AFLL | FCL | MCL | MCR | MAC | ML |
|---|---|---|---|---|---|---|

A message consists of one or more fragments. Each fragment shall be transported in one Data Link Layer frame. Table 13 provides an overview of all possible AFL Fields as shown in Figure 12.

**Table 13 – Overview of all AFL Fields**

| Size (bytes) | Field Name | Description |
|---|---|---|
| 1 | CI | Indicates that an Authentication and Fragmentation Layer follows. |
| 1 | AFLL | AFL-Length |
| 2 | FCL | Fragmentation-Control-Field |
| 1 | MCL | Message-Control-Field |
| 4 | MCR | Message-Counter-Field |
| 8 | MAC | Message-Authentication-Code |
| 2 | ML | Message-Length-Field |

The grey-shaded columns indicate optional fields. Their inclusion is defined by the Fragmentation Control Field specified in chapter 6.2.3.

### 6.2.2 AFL-Length Field (AFL.AFLL)

This Field describes the number of bytes within the AFL following the field AFL.AFLL.

**NOTE:** The AFL.AFLL+1 point to the first byte of the next layer within this datagram.

### 6.2.3 AFL Fragmentation Control Field (AFL.FCL)

The Fragmentation Control Field indicates size and presence of the following fields in the current fragment

**Figure 13 – AFL Fragmentation Control Field bitmap (AFL.FCL)**

| 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| RES | MF | MCLP | MLP | MCRP | MACP | RES | RES | FID | | | | | | | |

The fields AFL.AFLL and AFL.FCL are not part of the MAC protected message.

The bits in the AFL.FCL field define the presence of the respective field in the current fragment.

**Table 14 – AFL Fragmentation Control Field bitfield definitions**

| Bits | Field Name | Description |
|---|---|---|
| 15 | RES | Reserved |
| 14 | MF | More-Fragments<br>0 This is the last fragment<br>1 More fragments are following |
| 13 | MCLP | Message-Control in this Fragment Present |
| 12 | MLP | Message-Length in this Fragment Present |
| 11 | MCRP | Message-Counter in this Fragment Present |
| 10 | MACP | MAC in this Fragment is Present |
| 9, 8 | - | Reserved |
| 7 to 0 | FID | Fragment-ID. |

The Fragment-ID is used for the identification of each single fragment of a long message. Set FID to 1 for the first fragment of a fragmented message. FID shall incremented with each fragment. The FID shall never wrap around. [5]

### 6.2.4 AFL Message Control Field (AFL.MCL)

**Figure 14 – AFL Message Control Field bitmap (AFL.MCL)**

| | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|
| Name | RES | MLMP | MCMP | Res | AT | | ATO | |

[5] Because the maximum message length is 16 kByte and the fragment size is larger than 64 bytes, the Fragment-ID cannot wrap around.

**Table 15 – AFL Message Control Field bitfield definitions**

| Bits | Field Name | Description |
|---|---|---|
| 7 | RES | Reserved |
| 6 | MLMP | Message-Length in Message Present |
| 5 | MCMP | Message-Counter in Message Present |
| 4 | RES | Reserved |
| 3 | AT | Authentication-Type (see Table 16) |
| 2 | | |
| 1 | ATO | Authentication type options (Table 17) |
| 0 | | |

The bits 6 and 5 in the AFL.MCL field define the presence of the field in the message.

Table 16 and Table 17 describe the usage of the AT and the ATO-Field.

The AFL.MCL field shall always be present in the first fragment. It shall not be present in any following fragments of the same message.

**Table 16 – AT-Field of AFL .MCL**

| Bit 3 | Bit 2 | Description of AT-bit field |
|---|---|---|
| 0 | 0 | None |
| 0 | 1 | CMAC-AES128 (see 9.3.1) |
| 1 | 0 | Reserved |
| 1 | 1 | Reserved |

**Table 17 – ATO-Field of AFL .MCL**

| AT-Field | Bit 1 | Bit 0 | Description |
|---|---|---|---|
| 00b | 0 | 0 | Default value |
| | 0 | 1 | Not allowed |
| | 1 | 0 | Not allowed |
| | 1 | 1 | Not allowed |
| 01b | 0 | 0 | Reserved |
| | 0 | 1 | 8 bytes (see 9.3.1) |
| | 1 | 0 | Reserved |
| | 1 | 1 | Reserved for max. length |

## 6.2.5 AFL Message Length Field (AFL.ML)

This field declares the number of bytes following AFL.ML until the end of the unfragmented message.

**NOTE:** The Message length has to be calculated before the Message is separated in several fragments.

**Figure 15 – AFL Message Length Field bitmap**

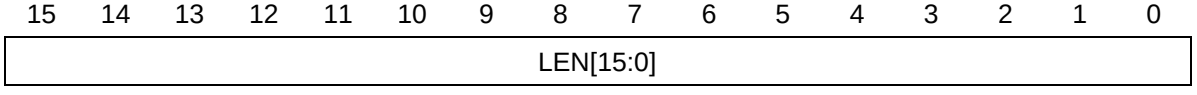


**Table 18 – AFL Message Length Field bitfield definitions**

| Bits | Field Name | Description |
|---|---|---|
| 15 to 0 | LEN | The message length shall be limited to 16 kbytes. The message length contains the sum of all TPL (see Table 1) fragments for one message. It does not include any AFL Fields. |

The AFL.ML Message Length Field shall only be present in the first fragment of a fragmented message to indicate the total message length. For single-fragment messages the AFL.ML shall not be used.

### 6.2.6 AFL Message Counter Field (AFL.MCR)

**Figure 16 – AFL Message Counter Field bitmap**

| 31 | 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C[31 to 16] | | | | | | | | | | | | | | | |
| 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| C[15 to 0] | | | | | | | | | | | | | | | |

**Table 19 – AFL Message Counter Field bitfield definitions**

| Bits | Field Name | Description |
|---|---|---|
| 31 to 0 | C | A 32-Bit Field, which is strictly monotonously increasing. The counter is incremented on every message-transmission. The counter never wraps. The initial value after manufacturing or after replacing the individual Master Key is 1. |

The AFL.MCR shall be present in messages from/to meters which are protected by security methods using the KDF. See 9.4.4 for details on the requirements for the Message Counter.

If the Message Counter Field is used, the AFL.MCR field shall always be present in the first fragment. It shall not be present in any following fragments of the same message.

### 6.2.7 AFL MAC-Field (AFL.MAC)

The length of the MAC field depends on the selected option AFL.MCL.ATO indicated by the AFL.MCL field.

If the MAC-Field is used, the AFL.MAC field shall only be present in the last fragment of a message.

Check chapter 9.1 for the presence of the AFL.MAC in messages from meter or gateway.

## 6.3 Conditions to apply an AFL

The AFL shall be applied

- In each datagram of a fragmented message (SND-UD, RSP-UD)
- In messages types with application data (SND-NR, SND-UD, RSP-UD) using Security profile B (see 9.1)
- In selected messages using Security profile C (see 9.1) with CMAC(refer to Annex F chapter F.2.3)

# 7 Combined Transport/Application Layer

## 7.1 Overview of Application Layers

The Application Layer has always a fixed frame structure as described in [EN 13757-3:2013]. It may transport either the meter Application Layer according to [EN 13757-3:2013] (M-Bus), or alternatively [FprEN 13757-1:2012] (DLMS/COSEM communication primarily used by electricity meters). Note that the CI field as the first byte of the combined Transport/ Application Layer distinguishes between these Application Protocol types and frame structures. A gateway or a consumer display shall be able to handle all Application Protocol types at least to the extent that it can extract the values required for its function or application from the message. This specification part covers mainly the M-Bus variant. Note that the gateway or the display needs to be able to parse any applied (M-Bus or COSEM or SML) Application Protocol into separate data points. However it is sufficient to “understand” i.e. de-code only the required values stated in chapter 8.

After the Transport Layer the Application Protocol starts immediately.

Possible Application Protocols for meter application data are:

- M-Bus (refer to 8.2)
- DLMS (refer to 8.3)
- SML (refer to 8.4)

Beside these Application Protocols for meter data exchange, there exist some more Application Protocols for special services:

- Clock Synchronisation Protocol (refer to 8.5)
- Application Error Protocol (refer to 8.6)
- Security Management Protocol (refer to Annex F)
- Alarm Protocol (refer to [EN 13757-3:2013] Annex D)
- and more (see Table 1)

## 7.2 Common Part for all combined Transport/Application Layers

### 7.2.1 General structure of the Transport Layer

The frame format of the combined Transport/Application Layer is the same for all Application Protocols. The Transport Layer starts with a CI-Field, which indicates the main message function and the type of coding (i.e. the Application Protocol) used for the rest of the message. After the CI-Field a fixed sequence of bytes follows, which is called header. There are 3 types of header.

The header structures are:

- No header:
  This header type is used on the wired M-Bus for unencrypted messages. The next byte after the CI-Field is the first byte of the selected Application Protocol.
- Short Header:
  The Short Header is used only for wireless M-Bus. If the message contains such a “short” header the meter identification is taken from the Link Layer (see chapter 3.1.3.1).
- Long Header:
  The Long Header is used both for wired and wireless M-Bus. If the message contains such a “long” header, this header contains (independent of transmission direction)

always the meter/actuator identification (see chapter 3.1.3.3). For the wired M-Bus it will be used in case of encryption.

Every Short/Long Header for wM-Bus contains:

- Access number
- Status Byte
- Configuration Field

Depending on the selected Encryption Mode in the Configuration field additional bytes (like Decryption-Verification) may follow, before the Application Protocol starts. The structure of the Transport and Application Layer is pictured in Annex D. Table 1 in chapter 2.2 list all supported CI-Fields and the related header type.

## 7.2.2 Access Number

### 7.2.2.1 Access Number for wM-Bus

The Access Number together with the transmitter address is used to identify a datagram. It will be distinguished between:

- Meter Access Number
- Gateway Access Number

The meter Access Number is generated by a meter/actuator. It shall be incremented by 1 (and only 1) with every synchronous transmission (refer to chapter 4.2.2.1). Asynchronous transmissions shall always apply the Access Number of the last synchronous transmission. The meter Access Number shall be applied to SND-NR, SNR-IR, ACC-NR and ACC-DMD datagrams. If a gateway accepts an ACC-DMD or an SND-IR from a meter/actuator it has to send an acknowledgement (ACK or CNF-IR) using the received meter Access Number. The received gateway Access Number has no impact on the stored meter Access Number of the meter/actuator. After power up of the meter its value of the Access Number shall be set by a randomized initial value from 0 to 255. The Access Number of the meter shall not be resettable.

If an Extended Link Layer exists (refer to 5.3) then the Access Number of the Extended Link Layer shall be used for the synchronous transmission and Link acknowledgement. Each datagram can be identified by the Access number of the Extended Link Layer. The additional Access Number of the Transport Layer may differ from the Access Number of the ELL. This Transport Layer Access number shall be used to indicate a new or old content of message. Each message can be identified by the Access number of the Transport Layer. The (first) response (RSP-UD) of a (fragmented) message shall contain the TPL-Access number of the concerning request (REQ-UD2) and the (last) acknowledgement (ACK) of a (fragmented) message shall contain the TPL-Access number of the concerning command (SND-UD).

**NOTE:** Other fragments may also contain Transport Layer (with the TPL-Access number) e.g. to provide an application error bit in the status byte.

The gateway Access Number is generated by the gateway. It may be selected without any restrictions. However the gateway shall not use the same Access Number for a new datagram to the same meter/actuator again within 300 seconds.

The meter/actuator shall not expect any specific order of Access Numbers in datagrams received from the gateway. It shall only distinguish between a new and an old datagram. The last received Access Number marks an old datagram. All other Access Numbers different from the last received one will be handled as the new Access Number. When the meter/actuator finishes the Frequent Access Cycle (refer to chapter 4.2.3) it shall clear the last received gateway Access Number. After that any received Access Number will be handled as a new one.

If the meter/actuator receives an SND-NKE, SND-UD, SND-UD2, REQ-UD1 or REQ-UD2, it shall use the received gateway Access Number of the ELL for its response or acknowledgement. The gateway may recognize an outstanding response or acknowledgement by its own Access Number. Hence the meter/actuator repeats the last response or acknowledgement, if the gateway has sent the request or the command with the old ELL-Access Number again. Otherwise it shall generate a new datagram with the new ELL-Access Number received from the gateway.

**NOTE:** These rules to apply the Access number for wireless M-Bus conforms to [EN 13757-3:2013].

#### 7.2.2.2 Access Number for M-Bus

For wired M-Bus the Access Number shall be conform to the [EN 13757-3:2013].

### 7.2.3 Status Byte

It will be distinguished between:

- Gateway Status (applied with CI-Field 5Ah, 5Bh, 60h, 61h, 64h, 65h, 6Ch, 6Dh or 80h)
- Meter Status (applied with CI-Field 6Eh, 6Fh, 72h, 74h, 75h, 7Ah, 7Ch, 7Dh, 7Eh, 7Fh, 8Ah or 8Bh)

The Meter Status and Gateway Status shall be as defined in [EN 13757-3:2013]. This standard defines in chapter 5.10 the meter status and in chapter 5.11 the gateway status.

The status field of the meter allows an Application Layer-response within an "ACK" message. (Note that this message itself only confirms the datagram reception). In this way, the bit "any application error" shall be used to communicate a failure during the interpretation or the execution of a received command. Note that more detailed error description may be provided by an application error message (refer to 8.6). Thus it is recommended to send a REQ-UD2 whenever the bit "any application error" is set.

It is recommended, that the Low Power bit is set 15 months before the intended end of operation.

Details about other error conditions like "permanent error" may be provided in Application Protocol (see chapter 8.2.4.2).

## 7.2.4 Configuration Field

### 7.2.4.1 General

The Configuration Field shall be used as specified in [EN 13757-3:2013]. It declares the method of data encryption (Encryption Mode) and the length of encrypted data. The Encryption Mode is a part of the Configuration Field declared by the bits MMMMM. The Encryption Mode is also responsible for the length of the Configuration Field and the meaning of all other bits (refer also 7.2.4.6). Table 20 shows the general structure of the Configuration Field and the position of the Encryption Mode.

**Table 20 – General definition of the Configuration Field**

| MS Bit 15 | Bit 14 | Bit 13 | Bit 12 | Bit 11 | Bit 10 | Bit 9 | Bit 8 | Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | LS Bit 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Mode specific | Mode specific | Mode specific | Mode bit4 | Mode bit3 | Mode bit2 | Mode bit1 | Mode bit0 | Mode specific | Mode specific | Mode specific | Mode specific | Mode specific | Mode specific | Mode specific | Mode specific |
| X | X | X | M | M | M | M | M | X | X | X | X | X | X | X | X |

**NOTE**: In OMS-Spec. Vol2. Issue 3.0.1 the applied Mode Field includes only bit8 to bit11. Bit12 was marked as reserved. From this version on the Mode Field includes the bits from bit 8 to bit 12.

For OMS only a few Encryption Modes are applied:

- Encryption Mode 0 (no encryption)
- Encryption Mode 5 (OMS standard for symmetric encryption)
- Encryption Mode 7 (OMS standard for advanced symmetric encryption)
- Encryption Mode 13 (OMS standard for asymmetric encryption)

**NOTE**: The Encryption Mode 4 is deprecated.

Chapter 9.2 describes the usage of these Encryption Modes. The next sub-sections describes the structure of the mode specific Configuration Fields.

### 7.2.4.2 Configuration Field for Encryption Mode 0

The structure of the Configuration Field of Mode 0 is identical to Encryption Mode 5 (refer to Table 21). The M and N has to be set to 00h to indicate that no encryption is applied. See also chapter 9.2.1.

### 7.2.4.3 Configuration Field for Encryption Mode 5

Encryption Mode 5 is a symmetric encryption method using AES128 with CBC, a special Initialisation Vector and a static key (see chapter 9.2.2).

The Initialisation Vector requires the usage of the Access Number. Be aware that the Initialisation Vector always shall apply the Access Number from Transport Layer whether or not the Extended Link Layer exists.

**Table 21 – Definition of the Configuration Field for Encryption Mode MMMM = 5**

| MS Bit 15 | Bit 14 | Bit 13 | Bit 12 | Bit 11 | Bit 10 | Bit 9 | Bit 8 | Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | LS Bit 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Bidirectional Communication | Accessibility | Synchronous | Mode bit4 | Mode bit3 | Mode bit2 | Mode bit1 | Mode bit0 | Number of encr. blocks | Number of encr. blocks | Number of encr. Blocks | Number of encr. blocks | Content of Message | Content of Message | Repeated Access | Hop Counter |
| B | A | S | M | M | M | M | M | N | N | N | N | C | C | R | H |

M is always 05h to mark AES128 with CBC and static key.

**NOTE**: A two byte sequence 0x2F, 0x2F (decryption verification) shall immediately follow the Configuration Field. The Decryption Verification Field is part of the Transport Layer.

**NOTE**: The Mode 5 may be used without Extended Link Layer and without Authentication and Fragmentation Layer (see 5.3.4).

### 7.2.4.4 Configuration Field for Encryption Mode 7

Encryption Mode 7 is a symmetric encryption method using AES128 with CBC and a dynamic key (see chapter 9.2.3). It is possible to identify up to eight different keys using the Key-ID.

The 3 byte Configuration Field (CF) to be used for Mode 0x07 is defined as follows:

**Table 22 – Configuration Field for Encryption Mode 7**

| MSBit 23 | Bit 22 | Bit 21 | Bit 20 | Bit 19 | Bit 18 | Bit 17 | Bit 16 | Bit 15 | Bit 14 | Bit 13 | Bit 12 | Bit 11 | Bit 10 | Bit 9 | Bit 8 | Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | LSBit 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Reserved | Reserved for Dynamic key | Dynamic key | Dynamic key | Reserved for Key-ID | Key-ID | Key-ID | Key-ID | Content of Message | Content of Message | Reserved for field extensions | Mode 4 | Mode 3 | Mode 2 | Mode 1 | Mode 0 | Number of encr. blocks | Number of encr. blocks | Number of encr. blocks | Number of encr. blocks | Reserved | Reserved | Reserved | Reserved |
| R | 0 | D | D | 0 | K | K | K | C | C | 0 | M | M | M | M | M | N | N | N | N | 0 | 0 | 0 | 0 |

M is always 07h to mark AES128 with CBC and dynamic key.

K selects the Key ID for Encryption. Only the use of K=0 (Master Key) is allowed. Other Key-IDs are reserved for future use.

D is 0x01 to mark Key Derivation Function as defined in chapter 9.4.

C declares the Content of Message according to [EN 13757-3:2013], Table 15 and Table 16.

N contains the number of encrypted 16 Byte Blocks for CBC Mode.

**NOTE**: A two byte sequence 0x2F, 0x2F (decryption verification) shall immediately follow the Configuration Field. The Decryption Verification Field is part of the Transport Layer.

**NOTE**: The usage of the mode 7 requires the Extended Link Layer (ELL), which covers the necessary Link Layer control elements like Hop Counter Bit, Synchronous Bit and Bidirectional Access Bit.

### 7.2.4.5 Configuration Field for Encryption Mode 13

Encryption Mode 13 is an asymmetric encryption method using TLS (see Annex F).

**Table 23 – Configuration Field for Encryption Mode 13**

| **MSBit 23** | **Bit 22** | **Bit 21** | **Bit 20** | **Bit 19** | **Bit 18** | **Bit 17** | **Bit 16** | **Bit 15** | **Bit 14** | **Bit 13** | **Bit 12** | **Bit 11** | **Bit 10** | **Bit 9** | **Bit 8** | **Bit 7** | **Bit 6** | **Bit 5** | **Bit 4** | **Bit 3** | **Bit 2** | **Bit 1** | **LSBit 0** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Reserved | Reserved | Reserved | Reserved | Protocol Type 3 | Protocol Type 2 | Protocol Type 1 | Protocol Type 0 | Content of Message | Content of Message | Reserved | Mode 4 | Mode 3 | Mode 2 | Mode 1 | Mode 0 | Number of encrypted bytes | Number of encrypted bytes | Number of encrypted bytes | Number of encrypted bytes | Number of encrypted bytes | Number of encrypted bytes | Number of encrypted bytes | Number of encrypted bytes |
| 0 | 0 | 0 | 0 | P | P | P | P | C | C | 0 | M | M | M | M | M | N | N | N | N | N | N | N | N |

M is always 0Dh (13 decimal) to declare an Encryption with TLS

**NOTE**: The applied TLS-Version can be retrieved from the TLS-Header

C declares the Content of message according to [EN 13757-3:2013], Table 15 and Table 16.

N contains the number of encrypted bytes. It indicates the number of bytes following the Configuration Field which are covered by the Protocol indicated by Protocol type (TLS). N is limited to 255.

**NOTE**: For larger sizes the exact number of bytes (minus the TLS header size 5 Bytes) can be found in the 4$^{th}$ and 5$^{th}$ Byte of the TLS header.

P defines the Protocol Type (refer to Annex F).

**NOTE**: No Decryption Verification Field follows the Configuration Field.

**NOTE**: The usage of the mode 13 requires the application of the Extended Link Layer.

### 7.2.4.6 Special bits of the Configuration Field

Bits CC are used to describe the content of the message

**Table 24 – Contents of meter message (from the meter/actuator to the gateway)**

| Conf. Bit 3 | Conf. Bit 2 | Contents of the message |
|---|---|---|
| 0 | 0 | Standard data message with unsigned variable meter data |
| 0 | 1 | Signed data message (consists of meter data with a signature approved for billing) |
| 1 | 0 | Static message (consists of parameter, OBIS definitions and other data points which are not frequently changed – see also 4.2.2.4). |
| 1 | 1 | Reserved for future extensions |

**Table 25 – Contents of gateway authentication (from the gateway to the meter/actuator)**

| Conf. Bit 3 | Conf. Bit 2 | Contents of data point authentication |
|---|---|---|
| 0 | 0 | Standard command message |
| 0 | 1 | Reserved for authenticated command message type 1 |
| 1 | 0 | Reserved for authenticated command message type 2 |
| 1 | 1 | Reserved for future extensions |

The declaration of the authentication methods helps the meter/actuator to detect the authentication method used by the gateway.

The Configuration Field of Encryption Mode 5 and 0 support the Link Control Bits B, A, S, R, and H. These bits are also provided by the Extended Link Layer.

If no Extended Link Layer exist then

- the bit S shall be used as described in chapter 4.2.2.1
- bits B and A shall be used as described in chapter 4.2.3.1
- bits H and R shall be used as describer in chapter 5.3.3.

Otherwise these Link Control Bits should always set to zero.

**NOTE:** If the ELL exists the Link Control Bits in the TPL have to be ignored (see 5.3.3).

The chapter 5.3.4 describes the conditions whether or not an Extended Link Layer exists.

## 7.3 Conditions to apply the Transport Layer

The Transport Layer is required for Messages types with application data. But also Message types without application data uses the TPL to provide following services:

- Meter address,
- Access number of the message,
- Reception level of the meter or
- Application error of the received message
- Encryption of application data

The meter/actuator shall apply the TPL for the Message types according to Table 26.

**Table 26 — Usage of TPL depending on Message type**

| Direction | Message type | Presence TPL wired M-Bus | Presence TPL wireless M-Bus |
|---|---|---|---|
| Master to slave | SND-NKE | Never | Always |
| | SND-UD | Optional [a] | Always [b] |
| | SND-UD2 | Not applicable | Always |
| | REQ-UD1 | Never | Always |
| | REQ-UD2 | Never | Always [b] |
| | ACK | Not applicable | Always |
| | CNF-IR | Not applicable | Always |
| Slave to master | SND-NR | Not applicable | Always |
| | SND-IR | Not applicable | Always |
| | ACC-NR | Not applicable | Optional [d] |
| | ACC-DMD | Not applicable | Always |
| | ACK | Never | Always [c] |
| | RSP-UD | Always | Always [b] |

[a] In case of encryption the TPL is necessary
[b] For a fragmented message sequence the TPL shall only be in the first datagram
[c] For a fragmented message sequence the TPL shall only be in the last datagram
[d] In case ELL is not there the TPL shall be provided (see 5.3.4)

# 8 Application Protocols

## 8.1 General requirements

### 8.1.1 Required Values and their Resolution and Accuracy

For the Open Metering System each message for billing purposes shall at least contain the current meter index with the meter accuracy and sufficient resolution for billing. Each message for consumer information shall contain sufficient information and accuracy to enable the gateway to display power respectively flow with sufficient accuracy and resolution.

For that reason the OMS-Meter shall be conform to Annex L.7 of [EN 13757-3:2013].

If power or flow values are transmitted and the applied averaging interval is smaller than the nominal transmission interval then the data point Averaging Duration should be transmitted additionally.

**NOTE:** The transmission of the Averaging Duration in the static telegram (refer to 4.2.2.4) will be sufficient.

## 8.2 M-Bus Application Protocol

The M-Bus Application Protocol is described in [EN 13757-3:2013]. To ensure interoperability, the use of the M-Bus Application Protocol in OMS is restricted by the following additional rules.

### 8.2.1 OMS-Data Point List

The Annex B list all harmonised M-Bus-Data points in the OMS-Data point list (OMS-DPL). This list consists of a VIB-Type List (VTL) and an M-Bus-Tag List. (MBTL)

The VIB-Type List provides all supported combinations of VIF's and VIFE's applied conform to this specification.

The M-Bus-Tag List provides all M-Bus-Tags applicable to conform to this specification. An M-Bus-Tag is an abstract presentation of a single M-Bus data point or a set of M-Bus-Data points which differs by the scaler (refer to VIB-Type List of Annex B) or resolution.

### 8.2.2 OMS-Gateway

OMS-Gateways shall support all M-Bus data points listed in the OMS-DPL (see Annex B).

The standard load profile and the M-Bus compact profile according to [EN 13757-3:2013], Annex I shall be supported, as well, provided that the underlying single M-Bus data points use the exact DIB/VIB coding given by the OMS-DPL. See Annex G for examples for the conversion of load profiles to single data points.

M-Bus data points compliant with [EN 13757-3:2013], but not listed in the OMS-DPL, may optionally be supported by OMS-Gateways.

### 8.2.3 OMS meter

Meters shall provide all M-Bus data points that are marked as mandatory (M) or alternative (Ax) in the OMS-DPL for the meter with the respective Device Type. The exact DIB/VIB coding given in the Annex B shall be used.

Note that a data point consisting of a combination of tariff, subunit, storage number, function code, final DIFE and VIFE shall be unique within a message.

**NOTE**: Several data points which differentiate for example by the data type (INT/BCD) only are not allowed.

At least one of the alternative data points (Ax – refer to OMS-DPL) marked with the identical number (x) shall be provided by the meter. If multiple alternatives are provided in one message, all data points shall provide the required accuracy and resolution.

If a Meter provides additional M-Bus data points marked as optional (O) in the OMS-DPL it shall use the exact DIB/VIB coding given there.

Meters may additionally use the standard load profile or the M-Bus compact profile according to [EN 13757-3:2013], Annex I. The underlying single M-Bus data points shall use the exact DIB/VIB coding given by the OMS-DPL. See Annex G for examples for the conversion of load profiles to single data points.

M-Bus data points that are listed in the OMS-DPL shall not be used in alternative or manufacturer specific sense.

Additional M-Bus data points that are not explicitly listed in the OMS-DPL, but complies with [EN 13757-3:2013], may optionally be provided by the OMS-meter. But these additional data points shall not be used as replacement of present data points in the OMS-DPL.

### 8.2.4 Usage of specific data points

#### 8.2.4.1 Date, time and intervals

For the averaging time interval of power or flow values the data point “averaging duration” shall be used (see 8.1.1).

For an uncorrelated transmission (refer to Annex L chapter L.7.3.4 in [EN 13757-3:2013] the elapsed time between measurement and transmission shall be coded with the data point “Actuality Duration”.

The nominal transmission interval used for synchronous transmission should be declared in installation datagrams (if available) with the data point “period of nominal data transmissions” (in seconds or minutes).

#### 8.2.4.2 Management data

Details about the error state indicated by Status Byte (refer to chapter 7.2.3) shall be coded with the data point “Error flags” or optional with “Error flags (standard)".

If a sequence number is needed (to prevent zero consumption – refer to [EN 13757-3:2013] chapter 5.9.2) it shall be coded as data point "Unique message identification”.

For meter management the reception level of a received radio device can be transmitted with the data point “Reception or noise level” (refer to [EN 13757-3:2013] Table 28, footnote d).

If this data point is used together with the Function field 10b in DIF it declares present quality limit of the reception level, which was exceeded by the received radio device. Example: 21h FDh 71h 9Ch marks a reception level > -100 dBm.

If this data point is used together with the Function field 11b it declares the typical noise level detected by this radio device. Example: 31h FDh 71h 9Fh means a noise level of -97 dBm.

### 8.2.5 OBIS code

The OBject Identification System (OBIS) defines the identification codes for commonly used data items in metering equipment.

These identification codes from DLMS-UA Blue Book are used for identification of:

- logical names of the instances of the Interface classes, the objects
- data transmitted through communication lines
- data displayed on the metering equipment

OBIS-codes in addition are used for the market communication of different contract partners for the standardised exchange of metering values. M-Bus coded metering data needs a mapping to the relevant COSEM object instantiation with OBIS code identifying the appropriate information. The Annex A defines a List of OBIS codes (LOC) as subset of M-Bus-Tags from the OMS-DPL and the assigned OBIS codes. An OMS-Gateway which is converting M-Bus data points to another Application Protocol shall add the respective OBIS code from the list.

If a meter/actuator uses an M-Bus data point which is not listed in the OMS-DPL, but is required for billing purposes, the OBIS declaration should be transmitted by the meter/actuator itself. A radio device should transmit this OBIS declaration by a static message (refer to 7.2.4.6). The OMS-Gateway then adds this OBIS declaration to the default OBIS conversion-table. The OBIS declaration via the M-Bus Application Protocol is described in [EN 13757-3:2013] Annex O.2.

## 8.3 DLMS Application Protocol

The DLMS Application Protocol for CEN meters is described in [FprEN 13757-1:2012], [EN 62056-6-1:2013] and [DLMS UA].

## 8.4 SML Application Protocol

The SML Application Protocol is described in document [SML-spec]. An example based on “SML - Smart Message Language” is listed in Annex N (Electricity meter).

## 8.5 Clock Synchronisation Protocol

The gateway shall provide the correct time (UTC) for every assigned bidirectional meter/actuator. As long as no encryption key of the meter is provided, the gateway may leave out the clock synchronisation for this meter/actuator. The clock synchronisation shall be provided periodically and on event. In the following cases a clock synchronisation shall be applied:

- Once every day (as long as the gateway has a valid time)
- When the gateway gets back to the valid time
- After the installation of a new meter or actuator
- After a communication interrupt for more than 24 hours

The clock synchronisation is a service of the gateway. The usage of this service depends only on the meter/actor itself and is not mandatory. The meter/actuator shall accept the synchronisation of the clock only if the time is transmitted in an encrypted way (valid for both wired and wireless communication).

The [EN 13757-3:2103] Annex H.3 describes the transmission of the clock synchronisation to the meter/actuator.

**NOTE**: The synchronisation of the meter clock may be in conflict with national laws.

## 8.6 Application Error Protocol

When a meter/actuator detects a failure during the interpretation or the execution of a received command it shall generate an application error. The presence of an application error should be announced in the Status field (see 7.2.3). The application error may be requested by the gateway with a REQ-UD2 as long as the Frequent Access Cycle is still active (refer to chapter 4.2.3). When the Frequent Access Cycle is over the meter/actuator shall discard the application error and reply the normal response to the next REQ-UD2.

The application error shall be transmitted with the generic Application Error Protocol as defined in [EN 13757-3:2013] chapter 8.3 (refer also Table 1 in 2.2).

Application errors 20h and 21h should be transmitted unencrypted.

NOTE: The Application Error Protocol can only be used for bidirectional communication.

# 9 Communication security

## 9.1 Overview

To protect the privacy of the consumption data of the consumer, all wireless communication with application data (all functions named ‘Command’ or ‘Response’ in Table 1) shall be encrypted. For wired communication an encryption of application data is optional.

With the usage of a MAC (see chapter 9.3) the integrity and the authenticity of the transferred data are ensured.

For some cipher methods an ephemeral key is derived from the original key. Such a key is called dynamic key. If the original key is directly used for the calculation of the encrypted payload or the Message Authentication Code then it is called static key.

Table 27 provides an overview about the supported security profiles. Each profile presents a valid combination of the encryption method, message authentication and the length and type of used key.

**Table 27 – OMS Security profiles**

| Profile | Encryption | Authentication | Key |
|---|---|---|---|
| No Security Profile | No encryption (ENC-Mode 0) [a] | No MAC (MAC-Mode AT=00b; ATO=00b) [b] | No key |
| Security profile A | AES128-CBC (ENC-Mode 5) [a] | No MAC (MAC-Mode AT=00b; ATO=00b) [b] | 128 bit static symmetric key |
| Security Profile B | AES128-CBC (ENC-Mode 7) [a] | CMAC (8 Byte trunc.) (MAC-Mode AT=01b; ATO=01b) [b] | 128 bit dynamic symmetric key (derived by KDF) |
| Security Profile C | TLS 1.2 (ENC-Mode 13) [a] | HMAC (TLS1.2) and additional CMAC (8 Byte trunc.) (MAC-Mode AT=01b; ATO=01b) [b] for communication establishment. | 256 bit elliptic curve key (384 bit optional) for TLS and 128 bit dynamic symmetric key (derived by KDF) for CMAC [c] |

[a] Declared in Configuration Field CF (refer to 7.2.4)

[b] Declared in AFL.MCL (refer to 6.2.4)

[c] During the TLS-handshake the usage of the CMAC is also required. However the normal data exchange of Mode 13 applies the HMAC of the TLS protocol for message authentication.

**Table 28 –Required Security profiles**

| Communication | OMS meter/actuator | OMS-Gateway |
|---|---|---|
| Wireless, unidirectional communication (according to 4.2) | Security profile A or Security profile B | Security profile A and Security profile B |
| Wireless, bidirectional communication (according to 4.2) | Security profile A or Security profile B or Security profile C | Security profile A and Security profile B and optionally Security profile C |
| wired communication (according to 4.1) | No security profile or Security profile A or Security profile B or Security profile C | No security profile and Security profile A and Security profile B and optionally Security profile C |

The manufacturer shall declare all supplied security profiles in data sheet of a meter/actuator or gateway.

**NOTE**: The asymmetric encryption (e.g. Security profile C) of bidirectional communication is necessary for certain countries due to national laws. It can provide a higher security level for transmissions where AES-based encryption with shared keys is not sufficient. Annex E provides a guideline of solutions that meet the known national requirements.

## 9.2 Encryption Modes

In order to support data confidentiality and to prevent zero consumption detection, encryption is required for all kind of communication which transports metering application data (refer to chapter 7.1). The encryption applies only to the Application protocol and the Decryption Verification (if present).

The Encryption Mode in use is indicated in the Configuration Field (see chapter 7.2.4).

### 9.2.1 No encryption with Mode 0

If Encryption Mode 0 selected then all following data are transmitted plain.

### 9.2.2 Symmetric encryption with Mode 5

Simple symmetric encryption is performed with mode 5. It uses AES-CBC with a static key of 128 bits and a specific dynamic Initialisation Vector based on the Access Number of the Transport Layer. The Encryption Mode is defined in [EN 13757-3:2013] chapter 5.12.6.

The data to be encrypted shall be padded to a multiple of 16 bytes before encryption. The padding value is 2Fh.

Annex N shows examples with both unencrypted and encrypted data.

### 9.2.3 Advanced symmetric encryption with Mode 7

Advanced symmetric encryption is performed with mode 7. It uses AES-CBC with a dynamic key of 128 bits and a static Initialisation Vector IV = 0 (16 Bytes of 0x00).

The dynamic key shall be generated with a Key Derivation Function (KDF) which is described in chapter 9.4.

For ensuring the integrity and authenticity the CMAC as described in chapter 9.3.1 shall be used.

Applying the Encryption Mode 7 always requires the usage of the AFL (see chapter 6), since the Message Counter C (see chapter 9.4.4) is needed for the KDF and transmitted in the AFL.

The data to be encrypted shall be padded to a multiple of 16 bytes before encryption. The padding value is 2Fh.

Annex N shows examples with both unencrypted and encrypted data.

### 9.2.4 Asymmetric encryption with Mode 13

Mode 13 describes an asymmetric encryption method based on Transport Layer Security (TLS). For details refer to Annex F.

**NOTE**: It should be noted that the TLS (Transport Layer Security) according to Security Profile C is independent from the KDF and CMAC, but the CMAC in the AFL offers the reliable transport and protection against DoS attacks for the TLS.

## 9.3 MAC-Generation

### 9.3.1 CMAC (AES 128 – 8 Byte truncated)

The authentication of the message is supported by the AFL (option AT=01b; ATO=01b - refer to 6.2.4) using the MAC. This MAC shall be calculated as specified in AES128 for Crypto-Message-Authentication (CMAC-AES128) according to [RFC4493]. The MAC shall be calculated as follows:

```
AFL.MAC = CMAC (Kmac/Lmac, AFL.MCL || AFL.MCR[7..0] ||
AFL.MCR[15..8] || AFL.MCR[23..16] || AFL.MCR[31..24] || {
AFL.ML[7..0] || AFL.ML[15..8] || } NextCI || ... || Last Byte of
message)
```

The presence of the AFL.ML field depends on the selection bits in the AFL.MCL field.

The MAC shall be calculated after the encryption. The MAC of a received message shall be verified before decryption.

An example is given in Annex N.

For a transmission from gateway to meter the key Lmac is used, for a transmission from meter to gateway the key Kmac is used (see key calculation in chapter 9.4.7).

The 16 byte result of this CMAC-function shall be truncated to 8 byte as defined in [RFC4493].

In deviation to the usual transmission order for octet strings on the M-Bus, the MSB of the MAC shall be transmitted as first byte, the LSB as last.

### 9.3.2 HMAC (TLS1.2)

The TLS1.2 requires an HMAC for the protection of the payload. This HMAC is within the TLS-protocol (within the APL). Refer to Annex F for details.

# 9.4 Key Derivation Function

## 9.4.1 General

The encryption of application data and the MAC shall be based on an ephemeral key, which is used for one message only. The ephemeral key shall be generated using the Key Derivation Function defined below. The Key Derivation Function shall also apply to the CMAC-Function according to [RFC4493]. There are 5 input values to the KDF specified in 9.4.2 to 9.4.6.

## 9.4.2 Individual Master Key (MK)

Before each transmission two ephemeral keys Kenc (for encryption) and Kmac (for authentication) are derived from the individual Master Key MK. There are two sets of key pairs (one set for the meter Kenc/Kmac and one set for the gateway Lenc/Lmac).

## 9.4.3 Derivation Constant (D)

The constant is used to derive different Keys for both Encryption and Authentication as well as for the two directions -from and to the meter.

**Table 29 – Constant D for the key derivation**

| D | Used for |
|---|---|
| 00h | Encryption from the meter (Kenc) |
| 01h | MAC from the meter (Kmac) |
| 10h | Encryption from the gateway (Lenc) |
| 11h | MAC from the gateway (Lmac) |

## 9.4.4 Message Counter (C and C')

The changing keys are generated by inclusion of a strictly monotonously increasing (non-secret) counter in the KDF. This counter is transmitted in the AFL.MCR field (see 6.2.6). The Message Counter maintained by the meter is named C, the Message Counter maintained by the gateway is named C'. The generation of C' is based on Message Counter C by adding an increment. The increment step shall not exceed the value of 100.

**NOTE**: Because of the short time window (2ms) for replying to a wM-Bus T-Mode datagram a gateway may calculate the Encryption Key and MAC Key in advance, based on the assumption of an Message Counter value (C').

An example for the handling of the Message Counter C and C' is provided in Annex J.

## 9.4.5 Meter-ID

For messages from the meter to the gateway which use a Short Header, (like CI=7Ah; see [EN 13757-3:2013]) the ID_0 to ID_3 corresponds to the LSB to MSB of the Link Layer Identification Number of the meter. For messages with long header (like CI=72h) the ID_0 to ID_3 corresponds to LSB to MSB of the Application Layer Identification Number of the meter.

For messages from the gateway to the meter the Long Header is always used. The ID_0 to ID_3 corresponds to the LSB to MSB of the Application Layer Identification Number (address) of the meter (not the gateway!).

### 9.4.6 Padding

To avoid the generation of the K2 (refer to [RFC4493]) in the KDF, the remaining bytes of the 16 byte block are filled with a padding sequence. For the generation of Kmac, Lmac and Kenc, Lenc the padding is fixed and consists of seven octets each containing the value of 0x07according to the rule that the input to the MAC shall be padded with 0x(16-l mod 16) bytes with value0x(16-l mod 16), where l equals the byte length of the input.

### 9.4.7 Key calculation

The calculation of Kenc and Kmac for the meter:

```
Kenc = CMAC(MK, 0x00 ||C[7..0] ||C[15..8] ||C[23..16] ||C[31..24]
||ID_0||ID_1||ID_2||ID_3||0x07||0x07||0x07||0x07||0x07||0x07||0x07)
Kmac = CMAC(MK, 0x01 || C[7..0] ||C[15..8] ||C[23..16] ||C[31..24]
|| ID_0||ID_1||ID_2||ID_3||0x07||0x07||0x07||0x07||0x07||0x07||0x07)
```

Where C[7..0] is the LSB and C[31..24] is the MSB (Big Endian) of the counter AFL.MCR.C from meter to other (gateway).

The gateway shall use a higher value C' than the last AFL.MCR.C received from the meter for the next message to the meter:

```
Lenc = CMAC(MK, 0x10 || C'[7..0] ||C'[15..8] ||C'[23..16] ||
C'[31..24] || ID_0 || ID_1 || ID_2 || ID_3 ||
0x07||0x07||0x07||0x07||0x07||0x07||0x07)
Lmac = CMAC(MK, 0x11 || C'[7..0] ||C'[15..8] ||C'[23..16] ||
C'[31..24] || ID_0 || ID_1 || ID_2 || ID_3 ||
0x07||0x07||0x07||0x07||0x07||0x07||0x07)
```

Where C'[7..0] is the LSB and C'[31..24] is the MSB (Big Endian) of the counter AFL.MCR.C from other (gateway) to meter.

Sequence for meter:

1. Increment C by one, Store C
2. Use C stored in the meter for derivation of next Kenc and Kmac
3. Generate message with AFL.MCR.C=C
4. Encrypt message with Kenc
5. Authenticate message with Kmac
6. Transmit message to gateway

Sequence for gateway after successful validation of C:

1. Use last received C from the meter (stored as CRx in the gateway) to generate incremented C'
2. Use C' for derivation of next Lenc and Lmac
3. Generate message with AFL.MCR.C=C'
4. Encrypt message with Lenc
5. Authenticate message with Lmac
6. Transmit message to meter

See Annex J for an example of Message Counter handling.

# Annex

## Annex A (Normative): List of OBIS codes for Basic Meters.

The List of OBIS-Codes provides a translation between an M-Bus-Tag and a relevant COSEM object instantiation with OBIS code identifying the appropriate information. This list is applicable when the M-Bus-data points are converted to another protocol.

This Annex may be subject to a more frequent update than this main document. Therefore the annex is not included. The current version (Release A or later) can be downloaded from the OMS Homepage (www.oms-group.org/en_downloads.html).

# Annex B (Normative): OMS-Data Point List

This Annex provides a list of all M-Bus-Tags supported by the OMS.

This Annex may be subject to a more frequent update than this main document. Therefore the annex is not included. The current version (Release A or later) can be downloaded from the OMS Homepage (www.oms-group.org/en_downloads.html).

# Annex C (Normative): Requirements on the gateway as a Physical M-Bus-Master

If equipped with an M-Bus master-interface the gateway shall meet the following requirements:

- Support a minimum of 6 unit loads i.e. max operating current: 6 × 1.5 mA + 20 mA (Space) = 29 mA
- Min. Mark voltage under mark/space current (max. 29 mA): 24 V
- Min. Space voltage under mark current (max. 9 mA): 12 V
- Resulting max. idle power: 24 V × 9 mA = 216 mW
- Baud rates: 300 and 2400 Baud
- Collision detect: For bus currents > 30 mA the bus voltage may drop below 24 V. Bus currents > 50 mA shall be signalled to the processor as a heavy collision state. This is required to support all the function of a wildcard-search.
- Galvanic isolation: As required in 4.3.3.9 of [EN 13757-2:2004]
- Symmetry as required in 4.3.3.10 of [EN 13757-2:2004]. DC symmetry requirements may be realized. This may be solved e.g. by a high resistance (2 × 1 MOhm) voltage divider. AC-symmetry may be realized via a (parallel) capacitive divider of e.g. 2 × 1 nF.

# Annex D (Informative): The Structure of the Transport and Application Layer

The fixed part after the CI-Field uses one of the following frame structures:

## D.1 No Header

The No Header may be used on wired M-Bus or for none OMS-messages. The Application Protocol starts immediately after the CI-Field.

### D.1.1 APL without Header

No message identification by Access Number, Status or encryption possible.

- Applied from master with CI = 50h; 51h; 52h;
- Applied from slave with CI = 70h; 71h; 78h

| CI | Data |
|---|---|

## D.2 Short Header

The Short Header can be applied if the meter application address is identical with the link address of the meter (wM-Bus).

### D.2.1 TPL/APL with Short Header

- Applied from master with CI = 5Ah; 61h; 65h
- Applied from slave with CI = 6Eh; 74h; 7Ah; 7Dh; 7Fh;

| CI | ACC | STS | CF | DV | Data |
|---|---|---|---|---|---|

**NOTE**: The Decryption Verification DV exists only in case of special Encryption Modes.

### D.2.2 TPL with Short Header

- Applied from slave with 8Ah

| CI | ACC | STS | CF |
|---|---|---|---|

## D.3 Long Header

If the meter application address differs from the link address of the wM-Bus Meter or if an wired M-Bus Meter used; then the Long Header with support of mandatory Secondary Address shall be applied.

### D.3.1 TPL/APL with Long Header

- Applied from master with CI = 53h, 5Bh; 60h; 64h; 6Ch, 6Dh
- Applied from slave with CI = 6Fh; 72h; 75h; 7Ch; 7Eh

| CI | Ident. No | Manuf. | Ver. | Med. | ACC | STS | CF | DV | Data |
|---|---|---|---|---|---|---|---|---|---|

**NOTE**: The Decryption Verification DV exists only in case of special Encryption Modes.

### D.3.2 TPL with Long Header

- Applied from master with 80h
- Applied from slave with 8Bh

| CI | Ident. No | Manuf. | Ver. | Med. | ACC | STS | CF |
|---|---|---|---|---|---|---|---|

## D.4 Legend:

| | |
|---|---|
| CI | Control Information Field |
| Ident. no | Identification Number (serial number) (part of meter address) |
| Manuf. | Manufacturer Acronym (part of meter address) |
| Ver. | Version (part of meter address) |
| Med. | Medium (Device Type) (part of meter address) |
| ACC | Access Number (from master initiated session uses gateway Access Number; from slave initiated session uses meter Access Number) |
| STS | Status (from master to slave used for gateway status (RSSI); from slave to master used for meter status) |
| CF | Configuration Field |
| DV | 2 Byte sequence 2Fh 2Fh for Decryption Verification |
| Data | Application data; coding depends on used Application Protocol |

# Annex E (Normative): Communication profiles for compliance with national regulations

A national law may require additional demands on the security of meter communication. This annex lists the applicable communication profiles in order to comply with the national regulation.

## E.1 Requirements for Smart Meter Gateways in Germany

The German law requires an approval for the operation of a Smart Meter Gateway in Germany. This approval checks both the security and the interoperability of a Smart Meter Gateway. The [BSI TR03109] describes the requirement to such a Smart Meter Gateway.

Such a Smart Meter Gateway has to reject an unsecure communication link to a smart meter. The Annex E.1 describes which services and security methods of the OMS-Specification shall be applied and which services are not allowed to conform to [BSI TR03109].

Annex E may be subject to a more frequent update than this main document. Therefore the annex is not included. The current version (Release A or later) can be downloaded from the OMS Homepage (www.oms-group.org/en_downloads.html).

# Annex F (Normative):
# Transport Layer Security (TLS) with wM-Bus

The German law requires TLS-protection for smart meters with bidirectional communication interfaces in the Local Metrological Network (LMN). The requirements to this interface are described in [BSI TR03109]. This Annex describes a BSI conform implementation of a TLS-communication on the wireless M-Bus.

TLS protected communication may also be used on wired M-Bus connections. However the wired M-Bus interface is not a mandatory interface of a Smart Meter Gateway according to [BSI TR03109].

Annex F may be subject to a more frequent update than this main document. Therefore the annex is not included. The current version (Release A or later) can be downloaded from the OMS Homepage (www.oms-group.org/en_downloads.html).

# Annex G (Normative): Examples for the conversion of Load Profiles to single data points

## G.1 Treatment of historical values in Compact Load Profiles with registers

Sets of historical billing values, indicated by the value group F (with F<255) of an OBIS-Code and assigned to dedicated COSEM objects, are always coded with a final DIFE with the value 00h. The number of DIFEs is variable. Such sets of historical billing values shall use a Compact Load Profiles with registers.

The final DIFE shall be used in the DIBs of all three related data points (Base Time, Base Value and Compact Load Profile with registers).

NOTE: Sets of historical billing values, indicated by the value group F (with F=255) of an OBIS-Code, like a Due Date Value, never use the final DIFE and apply the Compact Load Profile without registers.

## G.2 Exceptions

The Standard load profile and the Compact Load Profile are compatible to description of [EN 13757-3:2013], with one exception. In deviation to the standard this specification allows to have more than two DIFE's in the standard or compact profile. For the identification of Load profiles with registers it is sufficient that the end of DIB is marked with a final DIFE containing only 0.

## G.3 Data set of the Example

The following examples show how an original set of periodical consumption values is coded as Standard Load Profile or Compact Load Profile and how these Load Profiles are converted to a set of single M-Bus data points.

**Table G1– Example: Load profile of consumption values for a water meter**

| | | |
|---|---|---|
| 1st value at the end of the month | 2008-01-31 | 65 litres ($10^{-3}$ $m^3$) |
| 2nd value at the end of the month | 2008-02-29 | 209 litres |
| 3rd value at the end of the month | 2008-03-31 | 423 litres |
| 4th value at the end of the month | 2008-04-30 | 755 litres |
| Last value at the end of the month | 2008-05-31 | 1013 litres |

## G.4 Example for Standard Load Profile

**Table G2 – Example: Standard Load Profile composed of the periodical volume values**

| DIB | | VIB | Data | Hex coded (LSByte first) |
|---|---|---|---|---|
| Data field | Storage number | | | |
| 2 digit BCD | 8 | Size of storage block | 5 | 89 04 FD 22 05 |
| 2 digit BCD | 8 | Storage interval in months | 1 | 89 04 FD 28 01 |
| 16 bit binary | 12 | Date (Type G) | 2008-05-31 | 82 06 6C 1F 15 |
| 8 digit BCD | 8 | Volume (liters) | 65 | 8C 04 13 65 00 00 00 |
| 8 digit BCD | 9 | Volume (liters) | 209 | CC 04 13 09 02 00 00 |
| 8 digit BCD | 10 | Volume (liters) | 423 | 8C 05 13 23 04 00 00 |
| 8 digit BCD | 11 | Volume (liters) | 755 | CC 05 13 55 07 00 00 |
| 8 digit BCD | 12 | Volume (liters) | 1013 | 8C 06 13 13 10 00 00 |

**Table G3 – Example: Periodical volume values converted to single data points**

| DIB | | VIB | Data | Hex coded (LSByte first) |
|---|---|---|---|---|
| Data field | Storage number | | | |
| 16 bit binary | 8 | Date (Type G) | 2008-01-31 | 82 04 6C 1F 11 |
| 8 digit BCD | 8 | Volume (liters) | 65 | 8C 04 13 65 00 00 00 |
| 16 bit binary | 9 | Date (Type G) | 2008-02-29 | C2 04 6C 1D 12 |
| 8 digit BCD | 9 | Volume (liters) | 209 | CC 04 13 09 02 00 00 |
| 16 bit binary | 10 | Date (Type G) | 2008-03-31 | 82 05 6C 1F 13 |
| 8 digit BCD | 10 | Volume (liters) | 423 | 8C 05 13 23 04 00 00 |
| 16 bit binary | 11 | Date (Type G) | 2008-04-30 | C2 05 6C 1E 14 |
| 8 digit BCD | 11 | Volume (liters) | 755 | CC 05 13 55 07 00 00 |
| 16 bit binary | 12 | Date (Type G) | 2008-05-31 | 82 06 6C 1F 15 |
| 8 digit BCD | 12 | Volume (liters) | 1013 | 8C 06 13 13 10 00 00 |

**NOTE**: Corresponding table cells in Tables *G2* and *G3* are marked with corresponding background colours.

## G.5 Example for Compact Load Profile

**Table G4 – Example: Compact Load Profile composed of the periodical volume values**

| DIB | | VIB | Data | | | | | | Hex coded LS Byte first |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Spacing control byte | | | | | |
| Data field | Storage number | | LVAR | Increment mode | Spacing unit | Data field | Spacing value byte | Data | |
| 8 digit BCD | 8 | Volume (liters) | - | - | - | - | - | 65 | 8Ch 04h 13h 65h 00h 00h 00h |
| 16 bit binary | 8 | Format G | - | - | - | - | - | 2008-01-31 | 82h 04h 6Ch 1Fh 11h |
| Variable length | 8 | Volume (liters) | 10 | Incre-ments | Full month | 4 digit BCD | 254 | 144, 214, 332, 258 | 8Dh 04h 93h 1Fh 0Ah 72h FEh 90h 00h D6h 00h 4Ch 01h 02h 01h |

**Table G5 – Example: Periodical volume values converted to single data points**

| DIB | | VIB | data | Hex coded (LSByte first) |
|---|---|---|---|---|
| Data field | Storage number | | | |
| 16 bit binary | 8 | Format G | 2008-01-31 | 82 04 6C 1F 11 |
| 16 bit binary | 9 | Format G | 2008-02-29 | C2 04 6C 1D 12 |
| 16 bit binary | 10 | Format G | 2008-03-31 | 82 05 6C 1F 13 |
| 16 bit binary | 11 | Format G | 2008-04-30 | C2 05 6C 1E 14 |
| 16 bit binary | 12 | Format G | 2008-05-31 | 82 06 6C 1F 15 |
| 8 digit BCD | 8 | Volume (liters) | 65 | 8C 04 13 65 00 00 00 |
| 8 digit BCD | 9 | Volume (liters) | 209 | CC 04 13 09 02 00 00 |
| 8 digit BCD | 10 | Volume (liters) | 423 | 8C 05 13 23 04 00 00 |
| 8 digit BCD | 11 | Volume (liters) | 755 | CC 05 13 55 07 00 00 |
| 8 digit BCD | 12 | Volume (liters) | 1013 | 8C 06 13 13 10 00 00 |

**NOTE**: Corresponding table cells in Tables *G4* and *G5* are marked with corresponding background colours.

# Annex H (Informative): Gas Meter Consumption Data and their Coding

## H.1 Glossary

**Table H1 – Glossary of the Gas meter consumption data**

| | |
|---|---|
| $V_m$ | The volume at measurement conditions |
| $V_{tc}$ | Temperature converted volume |
| $V_b$ | The volume at base conditions |
| Measurement conditions | Conditions of the gas whose volume is measured at the point of measurement (e.g. the temperature and the pressure of the gas)<br>EN 12405:2002 3.1.2 |
| Base conditions | Fixed conditions used to express the volume of gas independently of the measurement conditions<br>EN 12405:2002 3.1.3 |
| Converted volume | The converted volume from the quantity measured at metering conditions into a quantity at base conditions. |

## H.2 Overview

For billing purposes the measured volume of a gas meter needs to be converted into energy. Depending on the technology of the gas meter there might be several parameters for this conversion:

- Temperature
- Pressure
- Gas calorific value

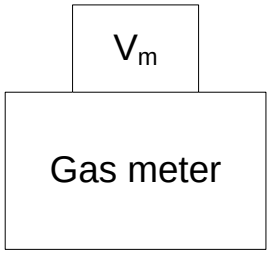
The conversion from the volume at measurement conditions ($V_m$) to the volume at base conditions ($V_b$) can be done by the gas meter, by a conversion device and/or by the billing system. Gas meter with build in temperature conversion device convert $V_m$ to $V_{tc}$.

In general mentioned conversions can be done explicitly using devices measuring the specific condition or also implicitly by meters that measure independently from the specific condition.

To inform the billing centre on possible conversions already done by the meter or a conversion device, the consumption data transmitted shall include a clear indication on both the conversion types and the base conditions to which the conversion is done. For meters with integrated or external conversion directly to energy the energy-oriented VIFs (e.g. “kWh”) together with the Device Type “gas” = 03h will provide such a clear indication which does not require further information.

## H.3 Volume at Measurement Conditions

All conversions are done solely at the billing centre, by assumption of measurement conditions that could not be measured, typically using legally defined gas temperatures and typical gas installations and/or installation height to take the pressure into account.




Note that the same coding is used for the raw, uncorrected original value if the meter internally corrects its volume accumulation for possible flow dependent errors since this will not influence the billing process.

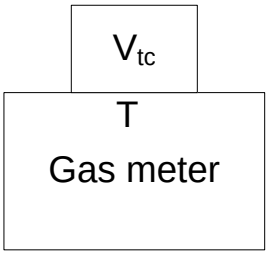
Suitable OBIS and M-Bus codes can be found in Annex A.

## H.4 Temperature Converted Volume $V_{tc}$

An individual meter based volume conversion to $V_{tc}$ (in contrast to the “global” billing centre based conversion) can be achieved either mechanically or electronically. It can be implemented either internally in the meter or by some external conversion device which then transmits converted values to the billing centre. Note that such a temperature conversion is based on a base temperature, which must be known to the billing centre. The default value for such a temperature at base conditions is 15 °C according to the [EN 1359:1998 + A1:2006].

If a meter uses a different base temperature its temperature at base conditions information shall be transmitted with each volume data message.

Note that meter data can be converted by the billing centre to its “billing temperature at base conditions” if this is different either from the default temperature of 15 °C or from the meters transmitted temperature at base conditions.




Suitable OBIS and M-Bus codes can be found in Annex A.

## H.5 Temperature and Pressure Converted Volume

In addition to a volume conversion just regarding temperature an individual meter might convert its measured volume to base conditions regarding temperature and pressure. To comply with standard conditions, which are usually stated by national regulations and to allow the creation of gas bills that can easily be understood by the consumer, the same temperature at base conditions shall be used as for the calorific value in the case when both temperature and pressure are converted.

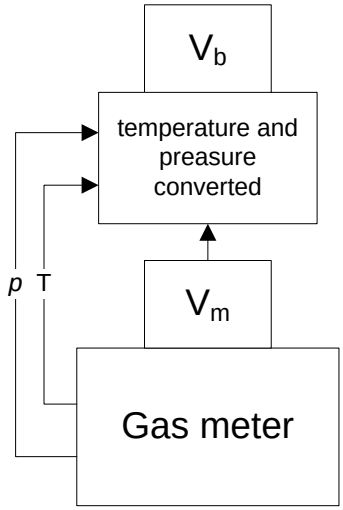
Devices complying with this do not need to send the information of the temperature at base conditions.

Note that a purely pressure converted volume, without temperature, is not supported.

Such a volume conversion is based on a pressure at base conditions, which must be known to the billing centre. The default value for such a pressure at base conditions is

1013.25 mbar. If a meter uses a different value for pressure at base conditions such pressure at base conditions information shall be added to each volume data message.

Note that meter data can be converted at the billing centre to its “billing pressure at base conditions” if this is different either from the default pressure of 1013.25 mbar or from the meter’s transmitted pressure at base conditions.




Suitable OBIS and M-Bus codes can be found in Annex A and Annex B.

## H.6 OBIS / COSEM Application of Physical Units for Gas

(Extract from [DLMS UA] Blue Book ed. 11)

Table H2 shows available physical units for the gas data objects given above. By application of a scale factor (ref. Table H3) the values can be scaled as required.

**Table H2 – Enumerated values for physical units**

| unit ::= enum | Unit | Quantity | Unit name | SI definition (comment) |
|---|---|---|---|---|
| (9) | °C | temperature (*T*) | degree-celsius | K - 273.15 |
| (13) | $m^3$ | volume (*V*)<br>$r_V$ , meter constant or pulse value (volume) | cubic meter | $m^3$ |
| (14) | $m^3$ | Converted volume | cubic meter | $m^3$ |
| (19) | l | Volume | litre | $10^{-3}$ $m^3$ |
| (23) | Pa | pressure (*p*) | pascal | $N/m^2$ |
| (24) | bar | pressure (*p*) | bar | $10^5$ $N/m^2$ |
| (52) | K | temperature (*T*) | kelvin | |

Some examples are shown in Table H3 below.

**Table H3 – Examples for scaler-unit**

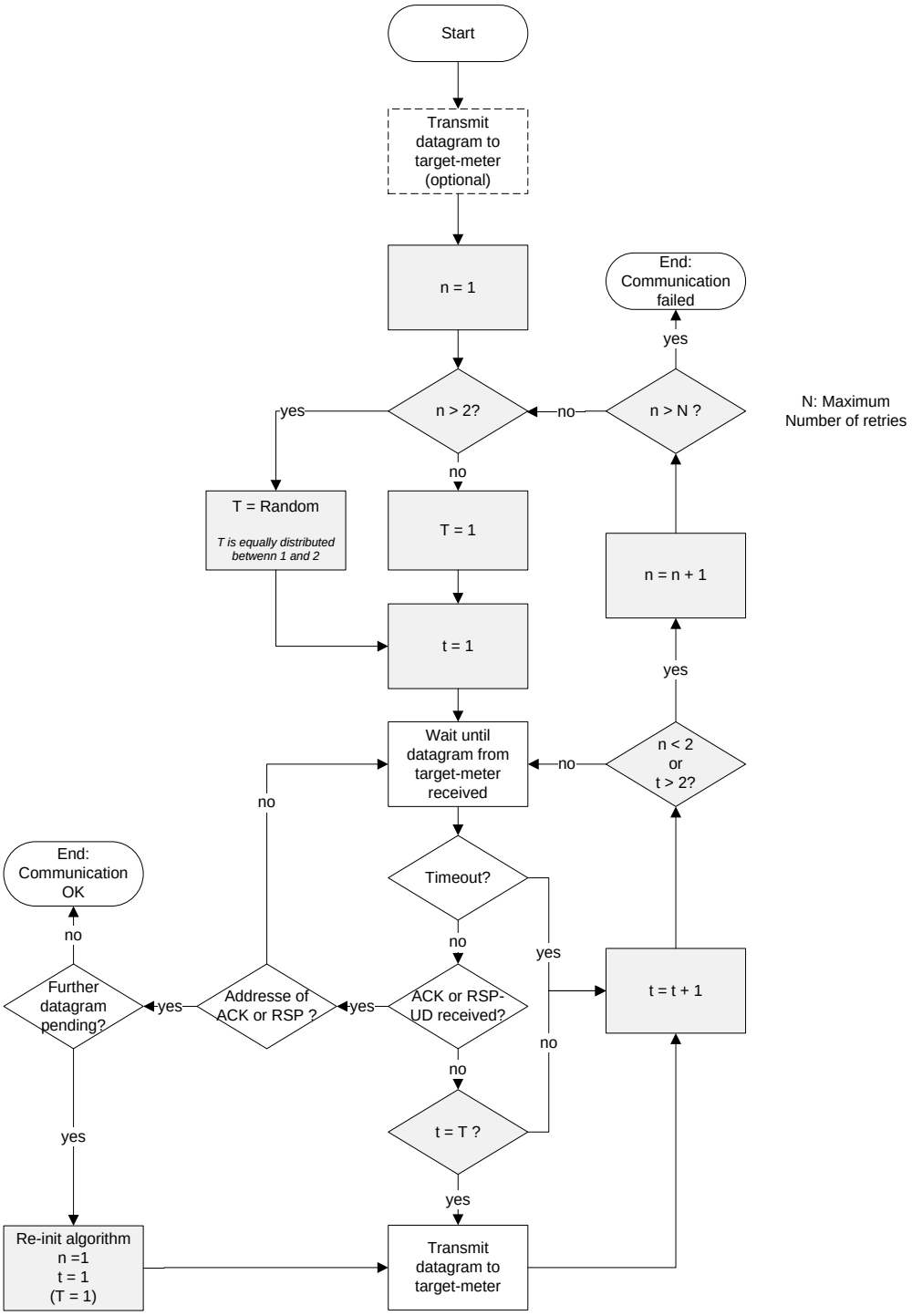
| Value | Scaler | Unit | Data |
|---|---|---|---|
| 263788 | -3 | $m^3$ | 263.788 $m^3$ |
| 593 | 3 | Wh | 593 kWh |
| 3467 | 0 | V | 3467 V |

# Annex I (Normative):
# Collision Avoiding Mechanism of the gateway

The following describes a mechanism for automatic retransmissions of interrogating devices in order to resolve collisions on the radio channel. The algorithm is based on a maximum number of N retries and choosing a random listen-after-talk-timeslot of the addressed meter. Furthermore it evaluates the received message types to prevent disturbing other conversations.

# I.1 Flowchart

**Figure I1 - Collision avoiding algorithm**



## I.2 Explanation

The flowchart shows the procedure to transmit a message to a bidirectional meter including the retry-mechanism. The parameter N gives the maximum number of retries.

The retry-algorithm applies three variables:

n Counts the number of tries to send the command

t Counts the number of datagrams received during the actual try

T Determines the datagram which will be followed by a transmission

In case of two unsuccessful tries resulting in n larger than 2, T is randomly chosen to 1 or 2 with a uniform distribution at the start of every (re-)try.

The basic idea is that within every try the interrogating device uses only one of two opportunities to transmit. This means that for both the first and second try the very first opportunity is used and for all following tries it would be either the first or the second one. The unused opportunity reduces the jamming-probability for competing devices and therefore contributes to a recovery of the overall-system.

A transmission to the addressed module is only performed under certain conditions. Of course, the general condition is the reception of a datagram from the target meter to meet the following listen-after-talk window. The algorithm evaluates furthermore, if the datagram is related to an already ongoing conversation, which is the case if the datagram is an acknowledgment or a response. In this case, it is further evaluated if this datagram is addressed to the interrogating device trying to send a transmission. If not, the device keeps on listening in order to leave this other conversation undisturbed. In case the ACK or RSP is dedicated to the device, the previous transmission is considered as successfully transmitted[6].

If the received datagram is neither part of another conversation nor the confirmation that a previous datagram was received, this would be an opportunity to send the datagram in case t equals T. Again, this latter additional condition resolves collision-scenarios with several devices transmitting simultaneously.

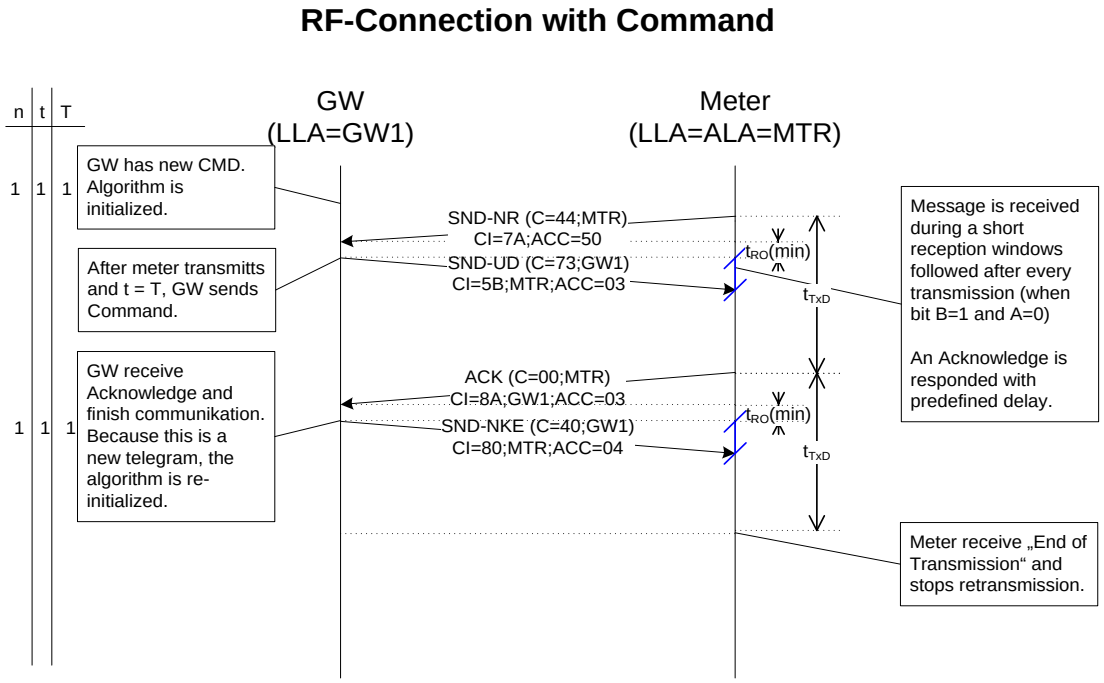
## I.3 Example: Access of one gateway without collision

Assume a scenario with only one gateway addressing a meter with a sufficient radio propagation in-between. The algorithm is initialized with n = 1, t = 1 and T = 1. As a consequence, the very first received datagram from the target meter is followed by the gateways transmission. An ACK by the meter, which should be received in a collision-free environment, confirms the reception and resulting in the transmission of the next datagram by the gateway. Therefore, compared to a system without the retry-mechanism, the performance in terms of latency or throughput is not influenced in any way.

The following flowchart shows this behaviour versus time together with the three variables of the algorithm.

[6] Based on the assumption, that the access-counter of the response can be used to match the answer of the interrogated module to the query.

**Figure I2 – Timing diagram without collisions**



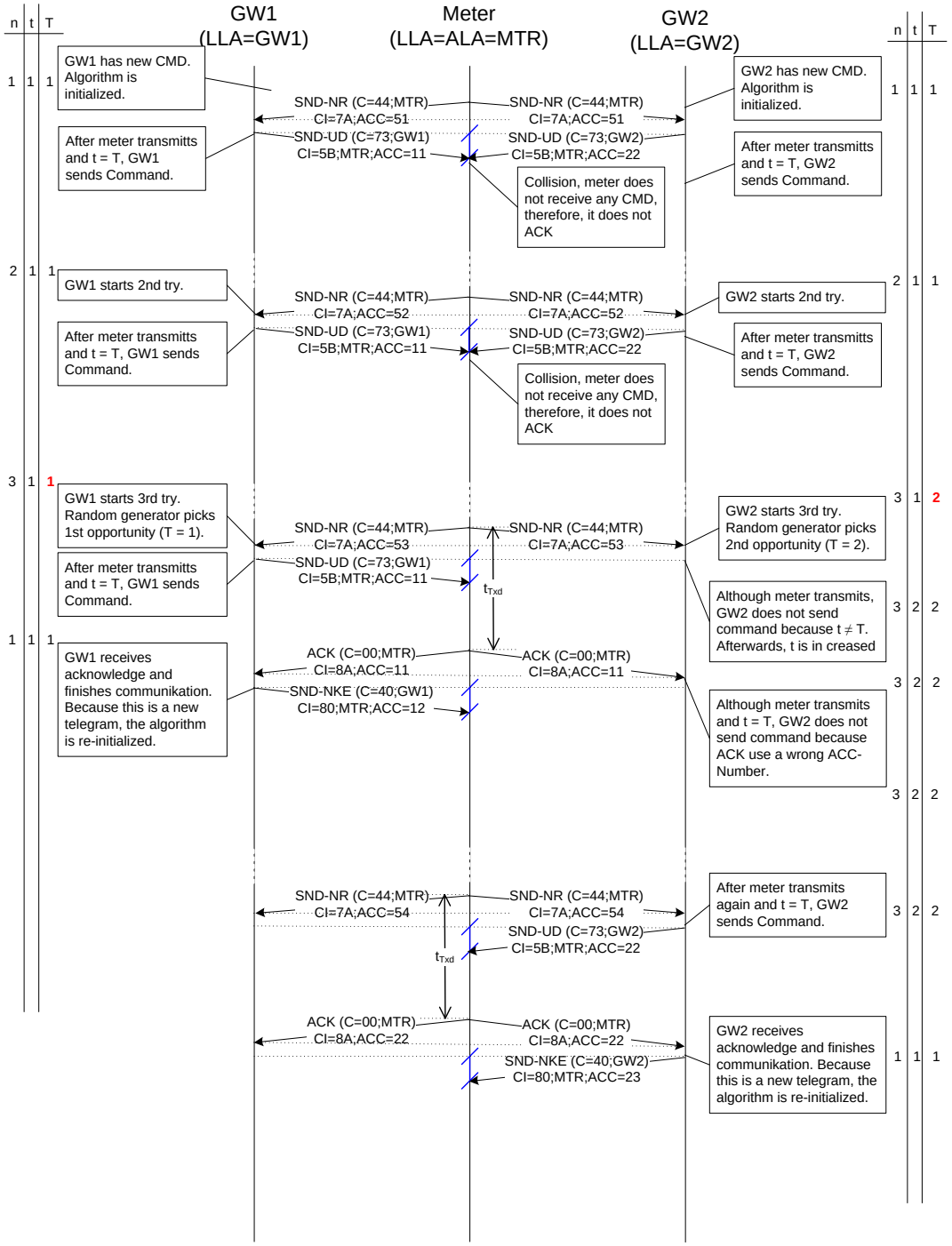

## I.4 Example: Access of two gateways with collision

Assume a scenario with two gateways and a meter, again with sufficient and equal radio propagation between the gateways and the meter. Due to some reason, on both gateways a command appears to be sent to the meter. Note that it cannot be sent immediately in case the meter's receiver is not always on. Therefore this scenario applies even in case of minutes between the appearances of the commands if the addressed meter has not transmitted since then, meaning that there was no opportunity to transmit the command.

Both gateways initialize the algorithm in the same way. In our assumption the received field strength of both gateways is equal at the meter and therefore the transmissions are jammed. Because the meter cannot receive any command in this case, there will not be an ACK by the module. Therefore the number of received datagrams during this first try is increased to 2. This furthermore results in starting the next try by increasing n from 1 to 2. Also for the second try, T is set to 1 (see flow chart) and therefore the very next opportunity is used, which again ends up in a collision. For the next try with n = 3, the random generator of every gateway determines T which now can be 1 or 2. Assuming a uniform distribution, there is a 50 % probability that two gateways choose different timeslots. This scenario is sketched in the following chart.

**Figure I3 – Timing diagram with collisions**

**RF-Connection with Command**




After the collision of the gateways' first transmission, both start a 3rd try with GW1 choosing the 1st and GW2 the 2nd opportunity. As a result, GW1 transmits the command after the next received datagram, whereas GW2 waits for the next possibility. Because the following transmissions of the meter are dedicated to GW1, GW2 does not take these opportunities, although t is equivalent to T. Note that the received datagrams dedicated to another conversation do not result in incrementing t (see the flowchart of the algorithm). After this conversation with GW1 is finished, GW2 takes the next datagram originating from the meter to transmit its pending datagram.

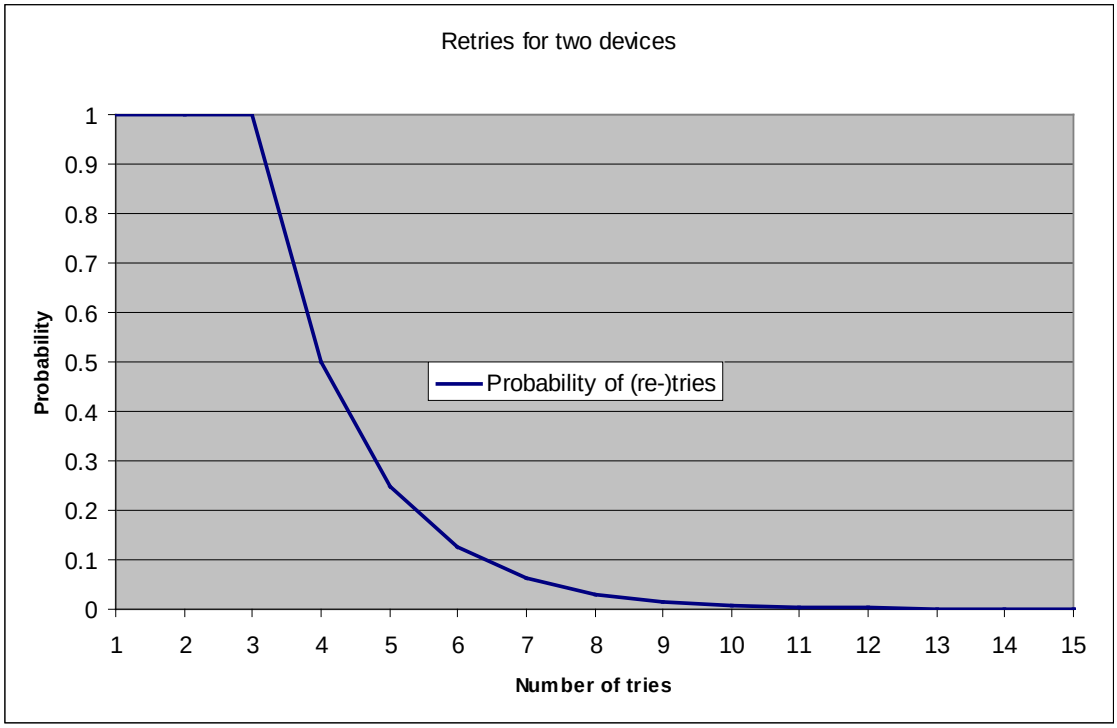
## I.5 Collision Probabilities

If more than one interrogating device wants to send a command at the same time, this results always in a collision during the first try. If there are two devices, the probability to get a collision during the $n^{th}$ try with n larger than 2 is $0.5^2 \times 2 = 0.5$.

$0.5^2$ is the probability that both devices choose the same opportunity and the multiplier 2 is reasoned by two possible opportunities. In general, the probability for collision is 1 in case of the first and second try and 0.5 for every other retries in case of two competing devices.

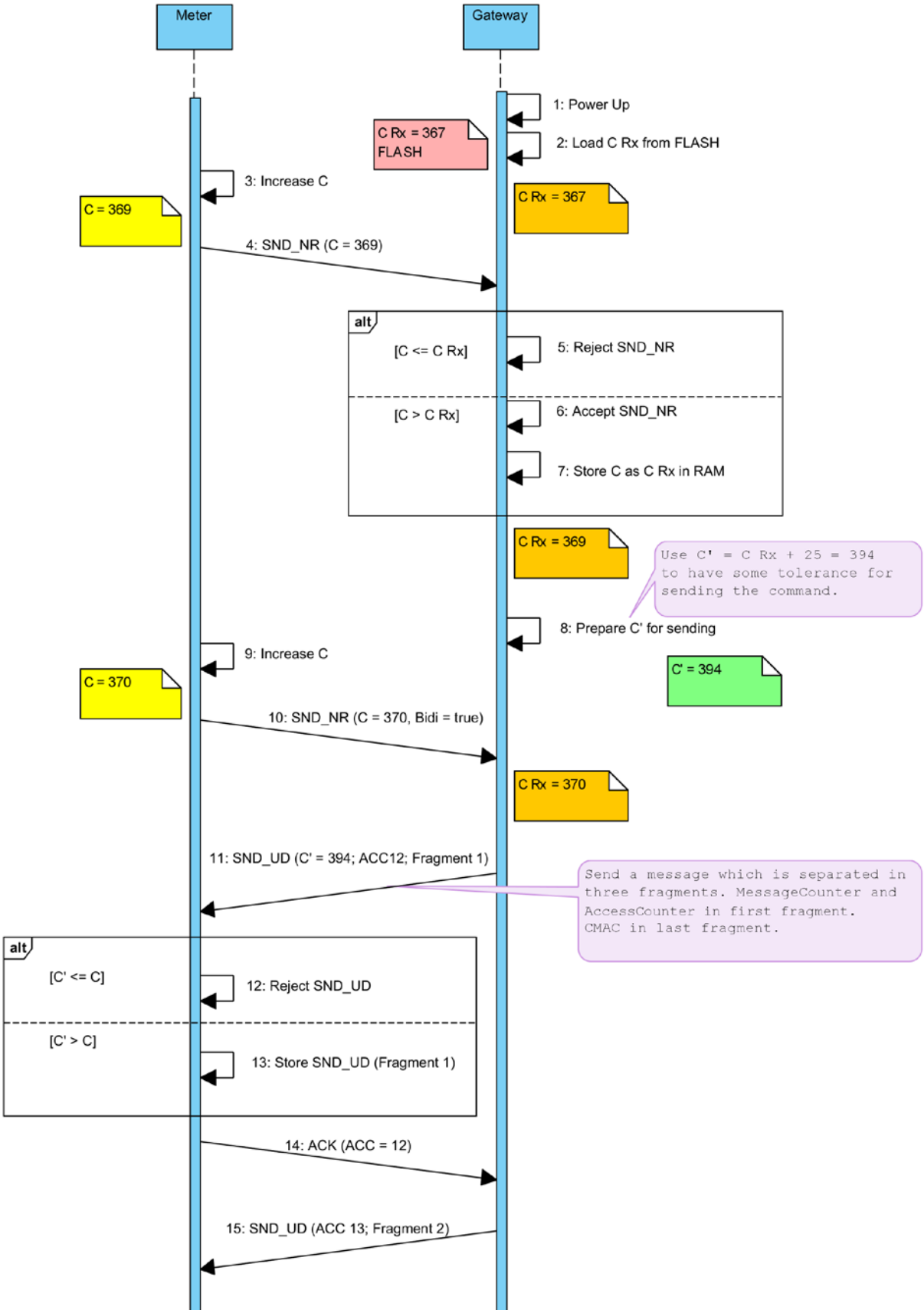
With the number of tries, the probability decreases that further tries are necessary. For example, the probability to have at least 3 tries is 1 and is the consequence of the 100 % collision probability for the $1^{st}$ and $2^{nd}$ try. The probability to have at least 4 tries is $1 \times 1 \times 0.5$ and therefore the result of having a collision in the $1^{st}$, $2^{nd}$ and $3^{rd}$ try. In general, the probability to have the necessity for at least n tries is $1 \times 0.5^{n-2}$ (for $n > 2$)

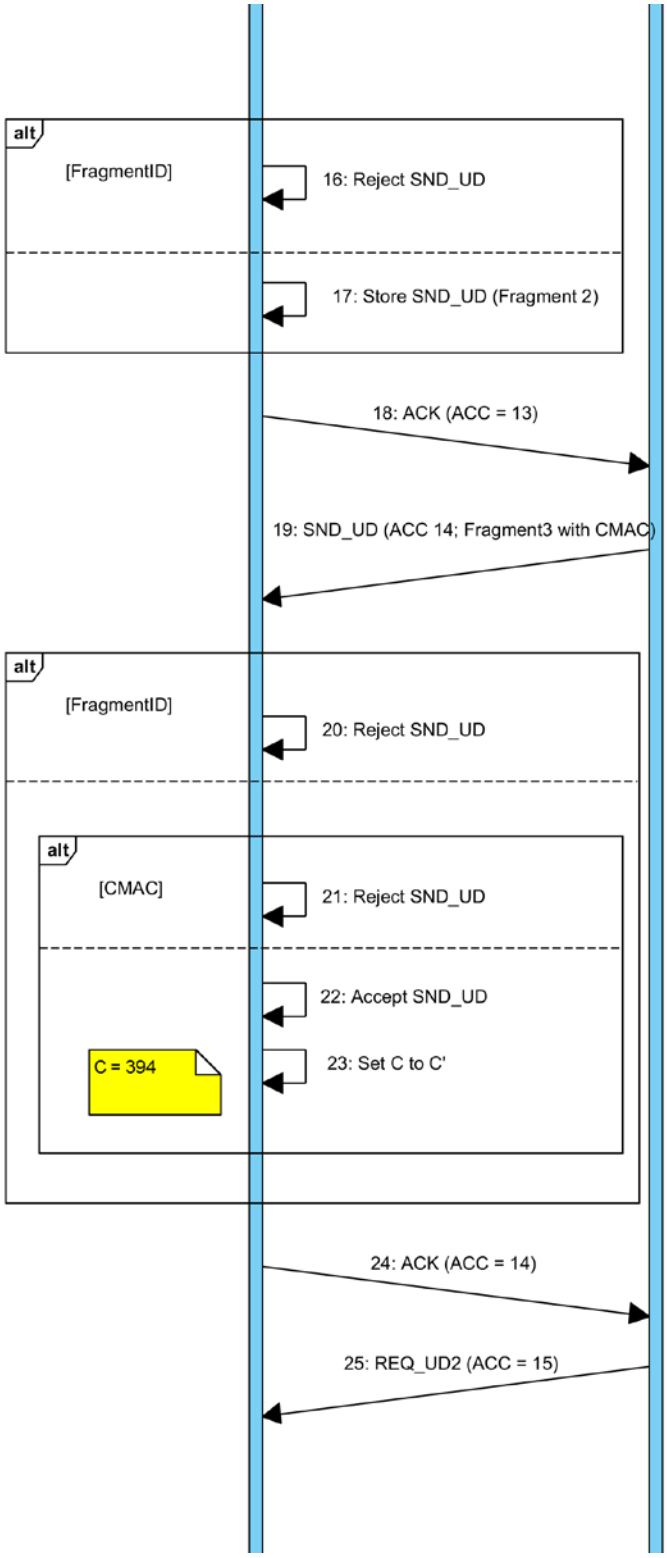
**Figure I4 – Collision probability**

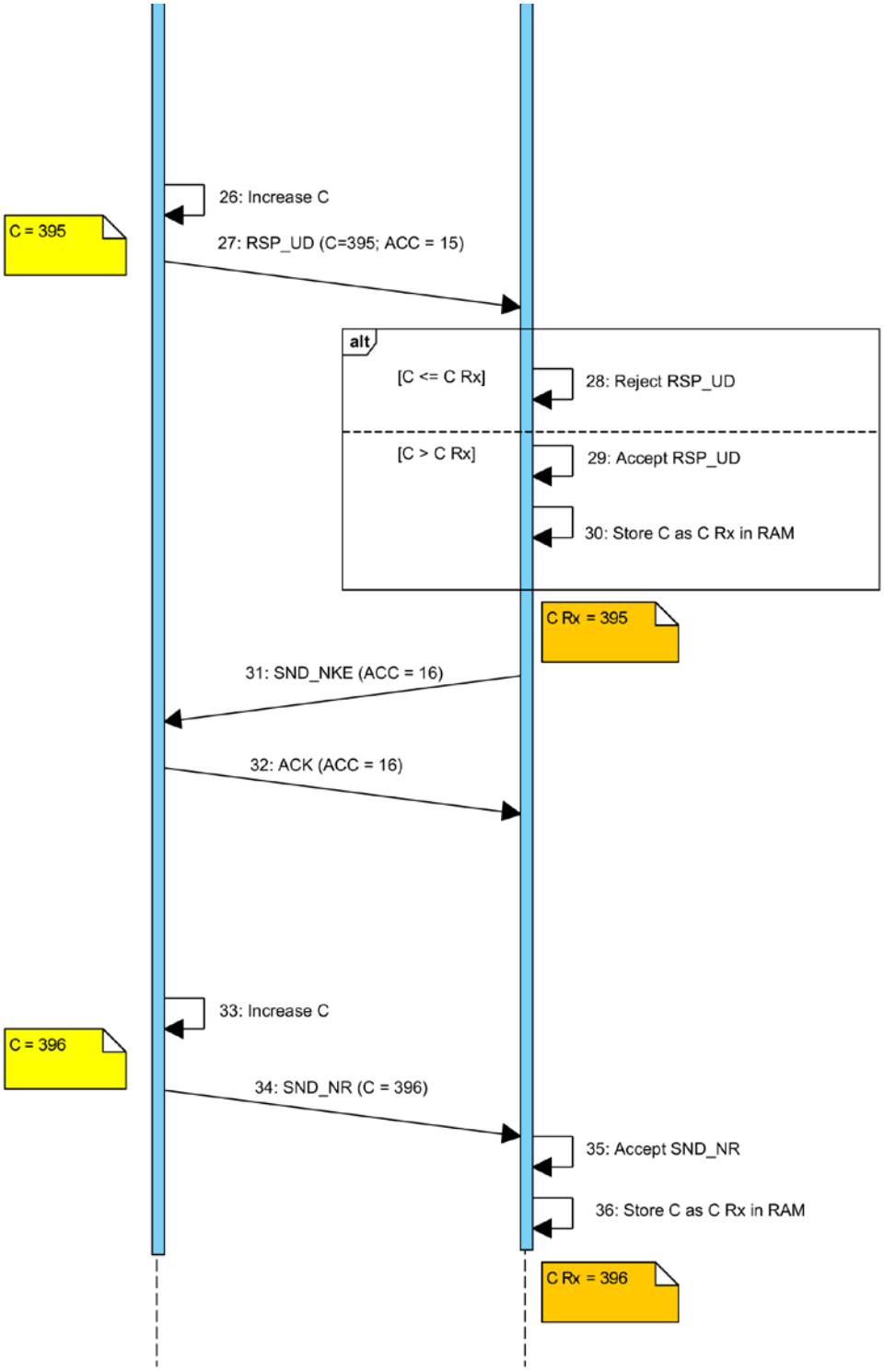



The probability for 12 tries or more is about 0.2 %, therefore a maximum number of N = 11 would be a suited limit for the proposed algorithm. This limits the number of opportunities to a maximum of $1 + 1 + 9 \times 2 = 20$.

# Annex J (Informative): Handling of Message Counter C/C'




alt
[FragmentID]
16: Reject SND_UD
17: Store SND_UD (Fragment 2)
18: ACK (ACC = 13)
19: SND_UD (ACC 14; Fragment3 with CMAC)
alt
[FragmentID]
20: Reject SND_UD
alt
[CMAC]
21: Reject SND_UD
22: Accept SND_UD
C = 394
23: Set C to C'
24: ACK (ACC = 14)
25: REQ_UD2 (ACC = 15)

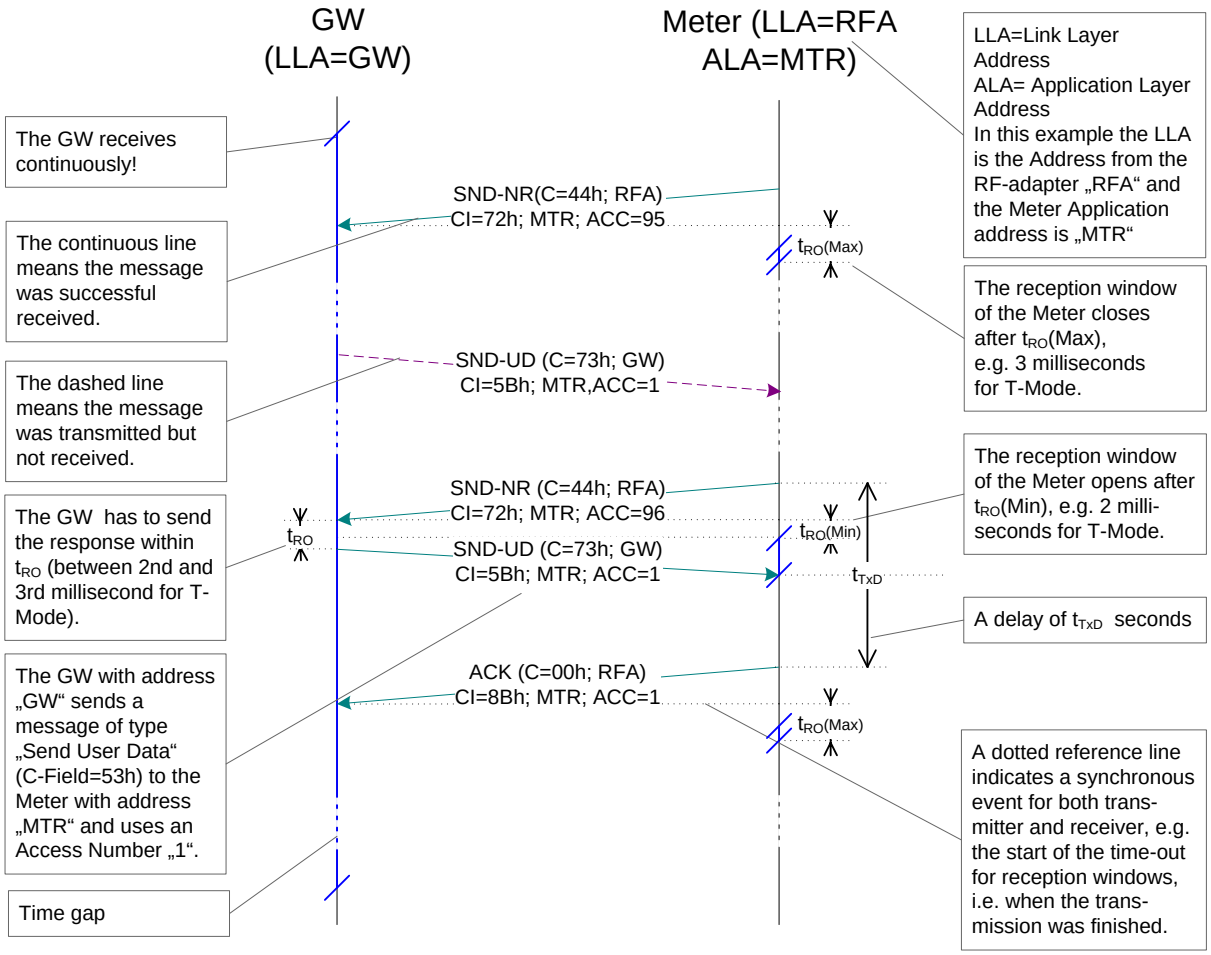

C = 395
26: Increase C
27: RSP_UD (C=395; ACC = 15)
alt
[C <= C Rx]
28: Reject RSP_UD
[C > C Rx]
29: Accept RSP_UD
30: Store C as C Rx in RAM
C Rx = 395
31: SND_NKE (ACC = 16)
32: ACK (ACC = 16)
33: Increase C
C = 396
34: SND_NR (C = 396)
35: Accept SND_NR
36: Store C as C Rx in RAM
C Rx = 396

# Annex K (Informative): Obsolete

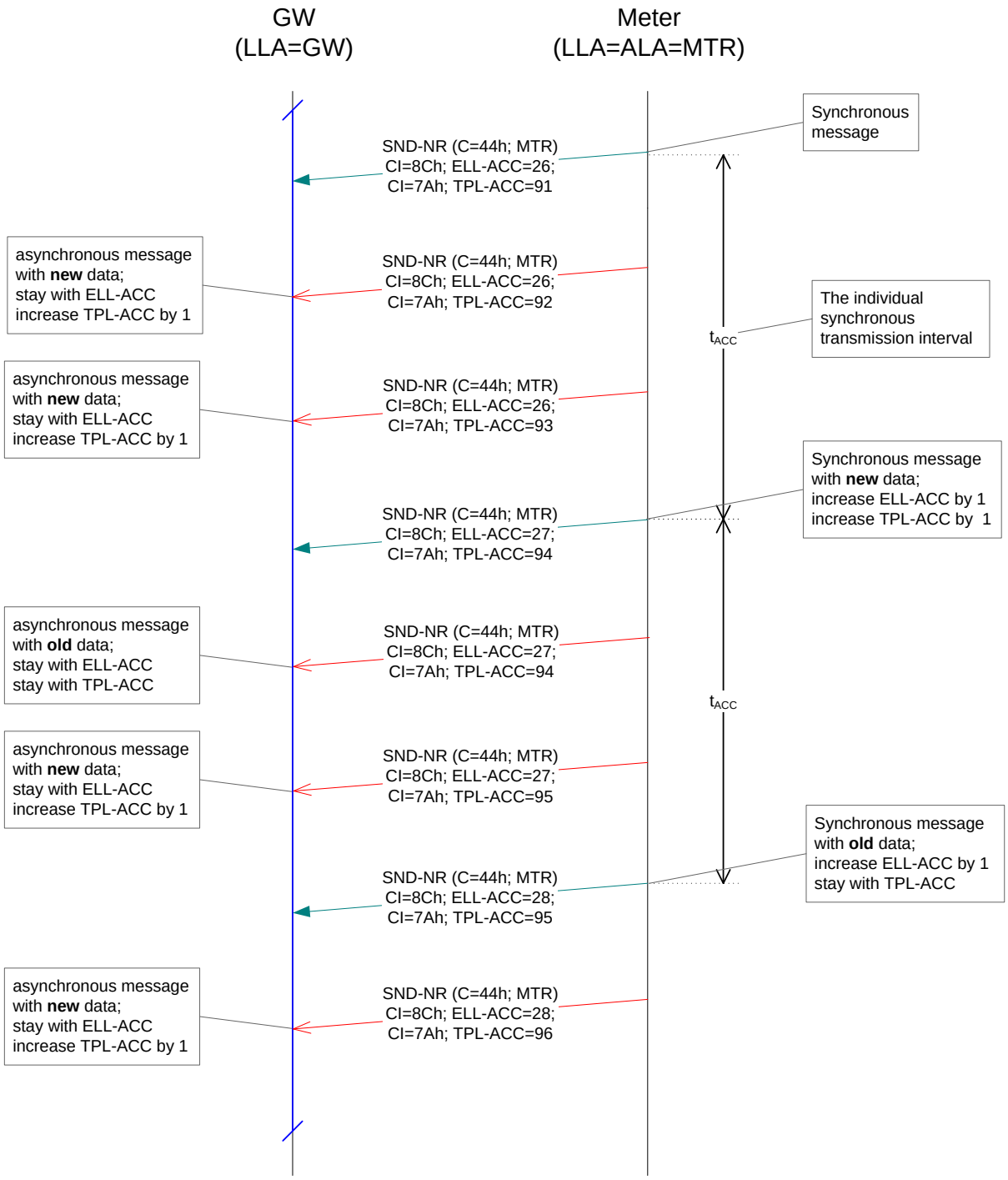
# Annex L (Normative): Timing Diagram

The next pages show examples of Timing diagrams. These are mainly examples of the S- and T-Mode. Examples of C-Mode are similar but differ slightly in the timing (refer to Annex E of [EN13757-4:2013]). If the Access number not explicit declared then the shown Access number is the Access Number of the ELL or of the TPL (if the ELL not exists).

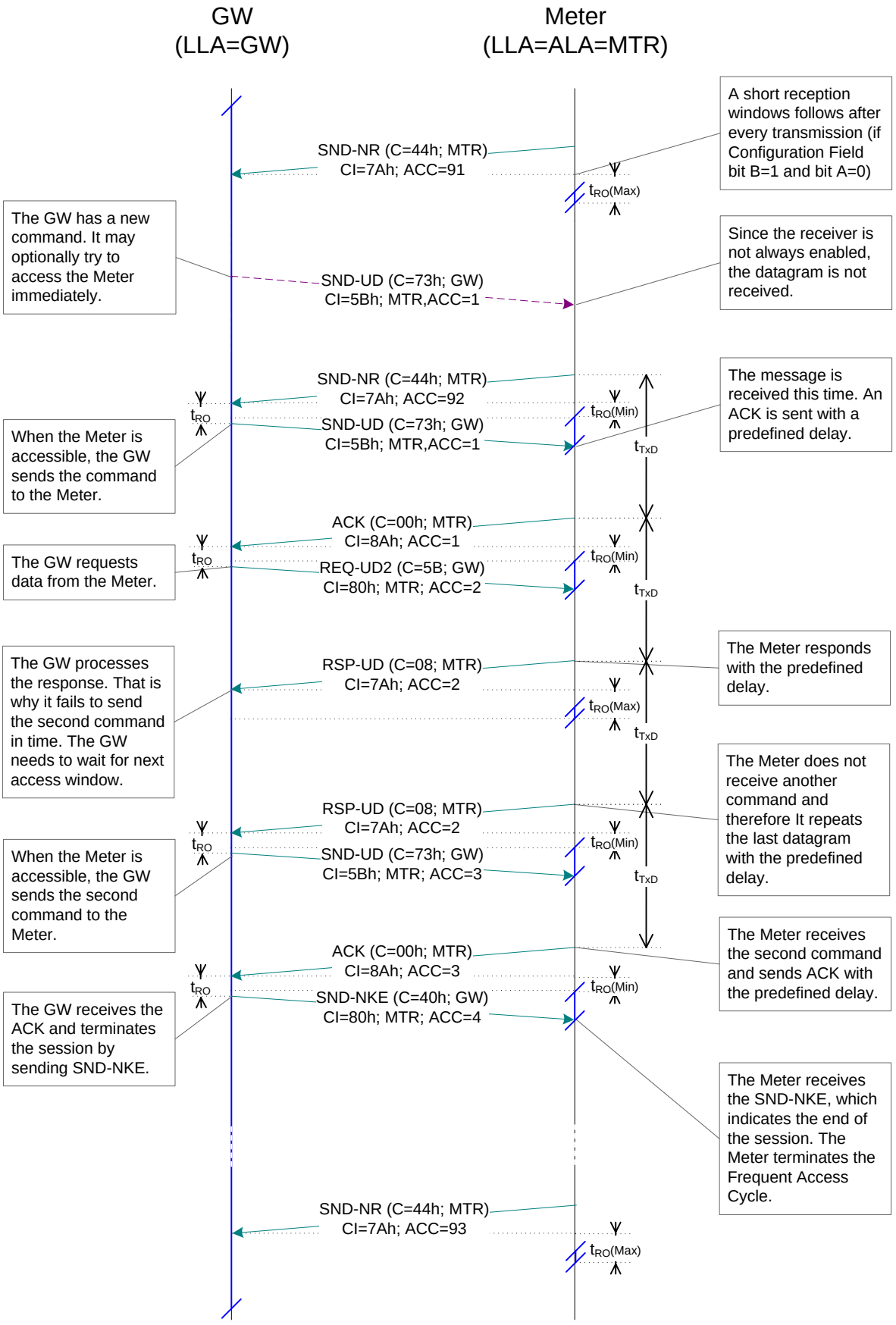
## Legend



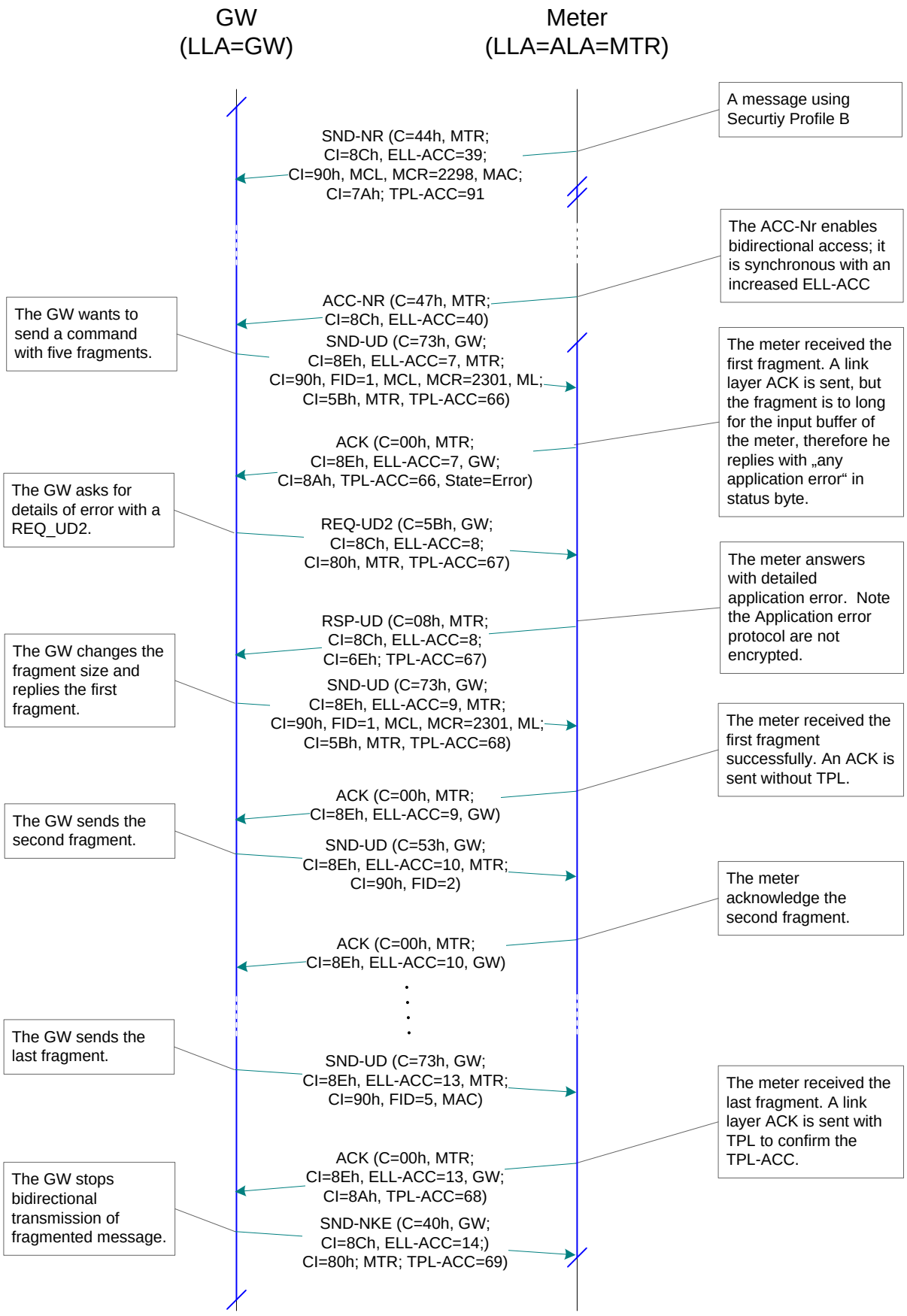
# Unidirectional meter with synchronous and asynchronous transmission



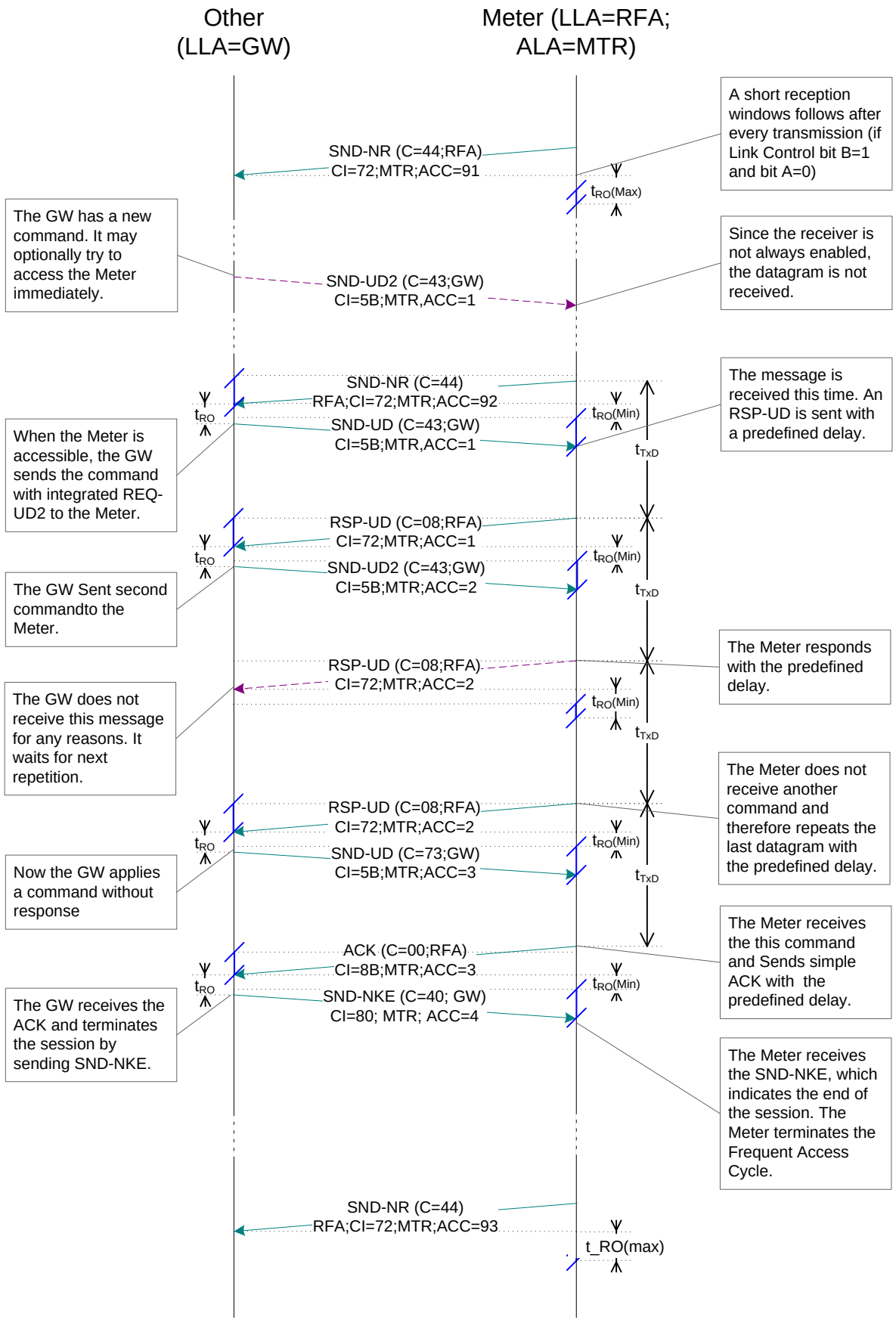
# RF-Connection with SND-UD and short TPL



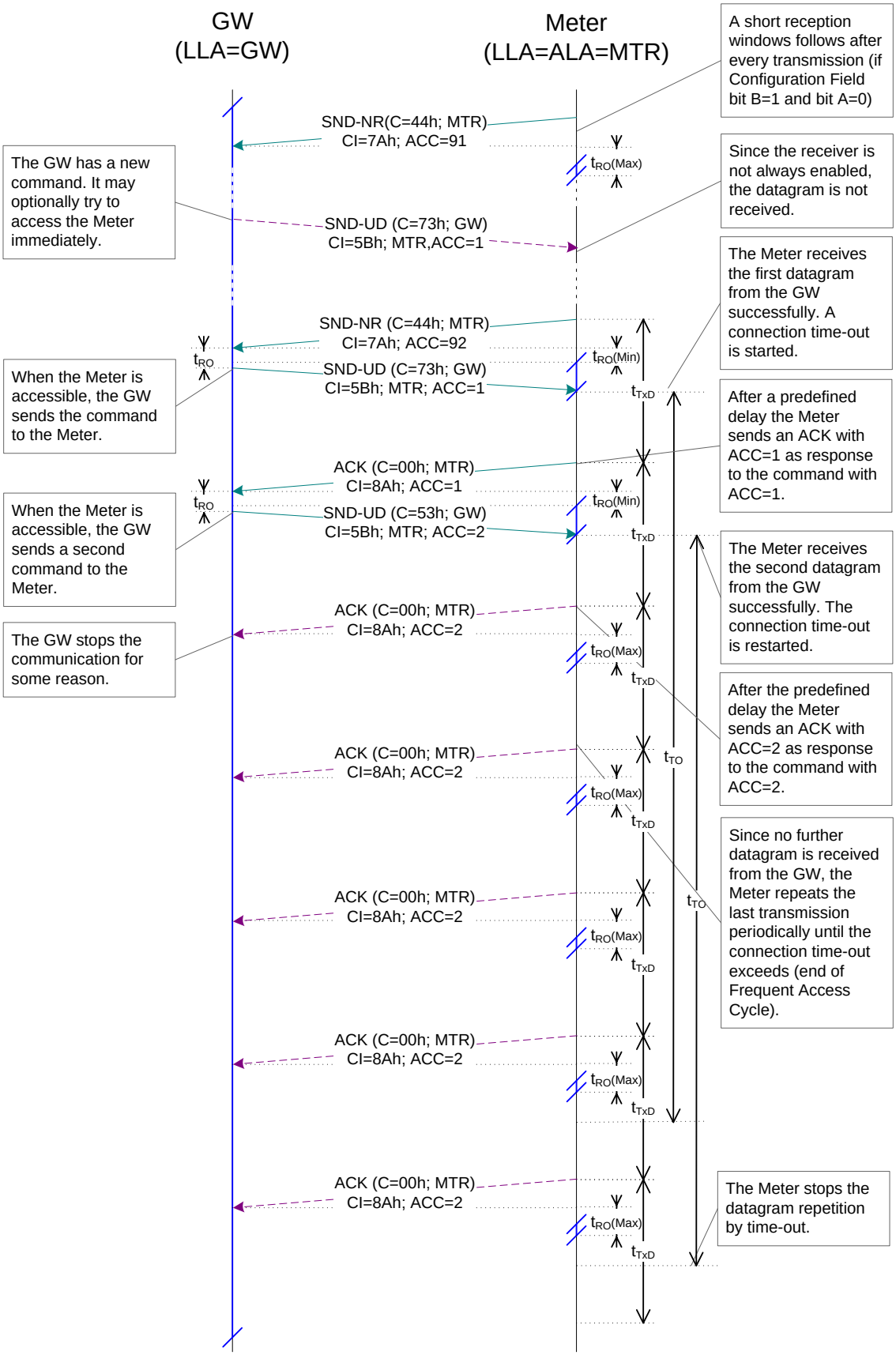
# Transmission of fragmented message with SND-UD



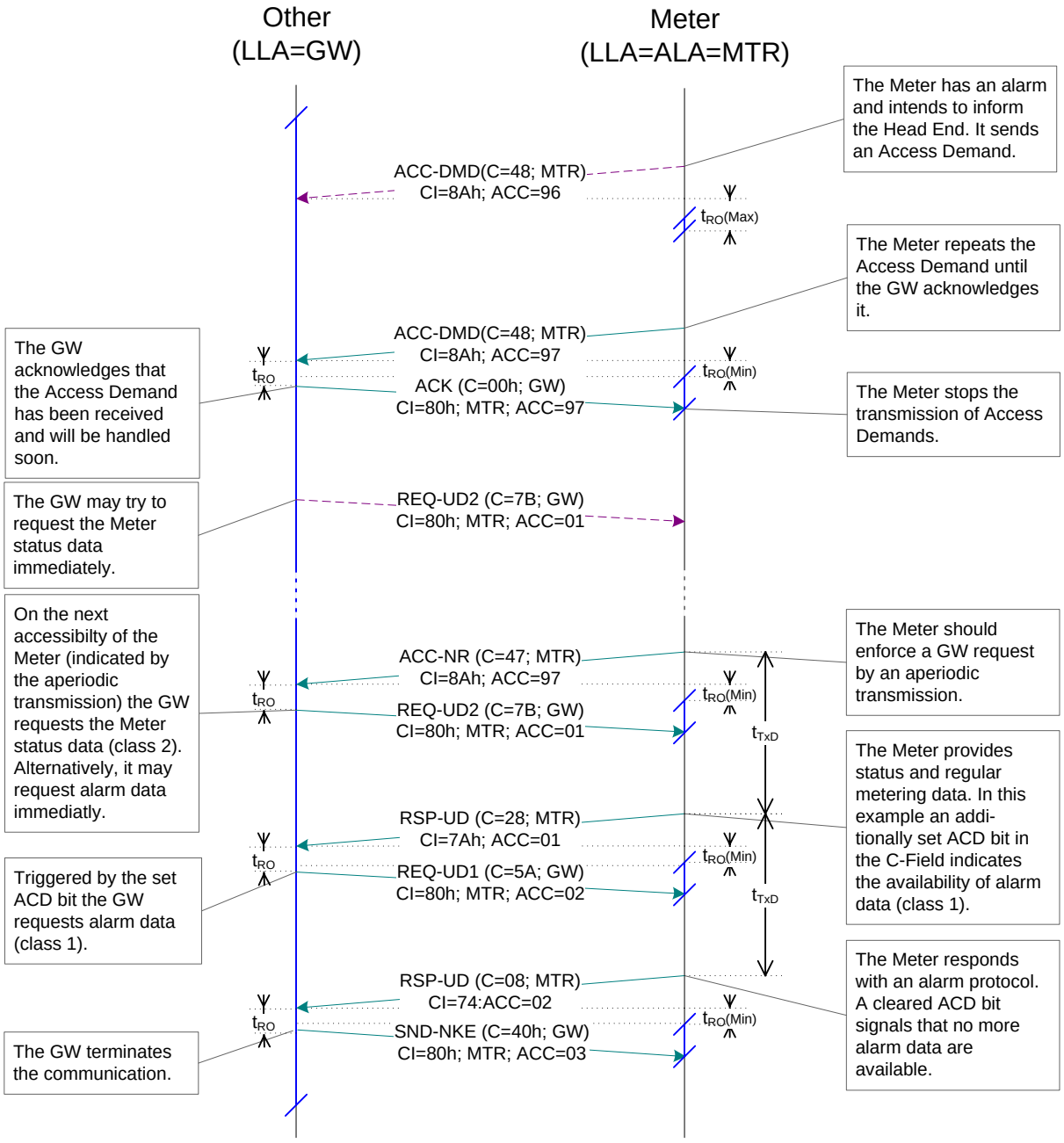
# RF-Connection with SND-UD2 and Long TPL



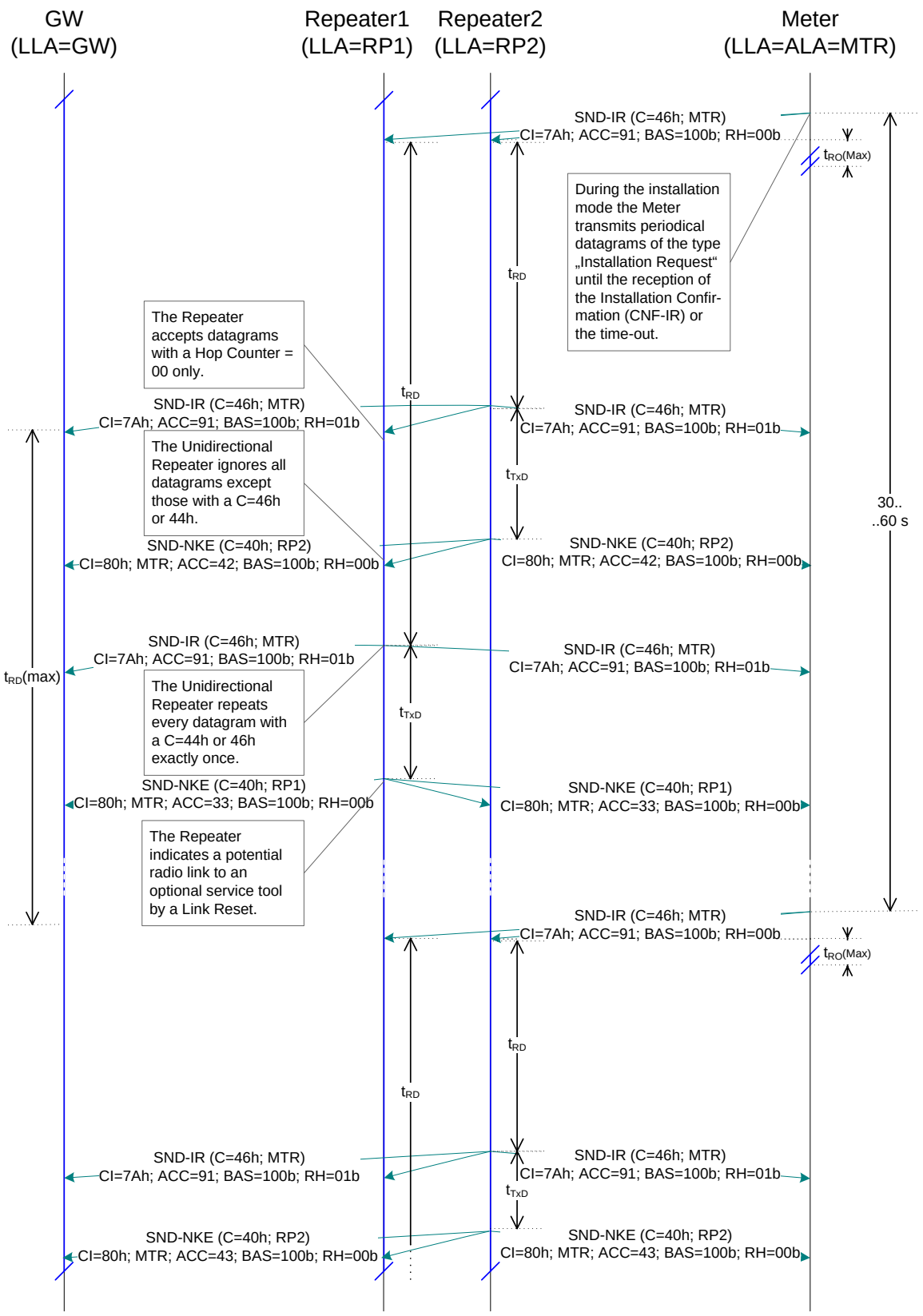
# Connection timeout of the Frequent Access Cycle



## Access Demand from Meter



## Installation Procedure with Unidirectional Repeaters



# Annex M (Informative): Obsolete

# Annex N (Informative): Datagram Examples for M-Bus and wM-Bus

This Annex list several message examples for wired and wireless M-Bus. Be aware this is an informative annex. In case of deviation between this annex and the normative specification, the content of specification has to be applied.

For the sake of better readability this annex is not included.

The current version (Release A or later) can be downloaded from the OMS Homepage (www.oms-group.org/en_downloads.html).

# Annex O (Informative): Alternative Physical Layers for OMS

Countries outside the CEPT may have defined other frequencies than those covered in the OMS-PC. OMS gives a recommendation on the usage of alternative Physical Layers and the country specific parameters.

Annex O may be subject to a more frequent change than this main document. Therefore the annex is not included. The current version (Release A or later) can be downloaded from the OMS Homepage (www.oms-group.org/en_downloads.html).