OMS

Open Metering System
Specification

Volume 2
Primary Communication

Issue 2.0.0 / 2009-07-20

Release

Document History

Version	Date	Comment	Editor
0.1	2008-02-12	Initialisation version for discussion in Open Metering Meeting 2008-02-26/26 in Laatzen	P. Gabriel, IMS <peter.gabriel@ims.fraunhofer.de>
0.2	2008-03-05	split into three documents first changes after review	P. Gabriel
0.3	2008-03-06	Changes after mini review with Mr. Pahl and Mr. Guderjahn, integrated OpenMetering7 (contributed by Prof. Ziegler)	P. Gabriel
0.4	2008-03-18	Changes after first review and review of version 0.3	P. Gabriel
0.5	2008-03-28	Changes after comments by members and correction of the english texts	P. Gabriel
0.6	2008-04-02	Further correction	P. Gabriel
0.7	2008-04-28	Takeover	H. Ziegler
0.8	2008-05-21	Result of Koblenz 2008-04-30	H. Ziegler
0.9	2008-05-26	Formating and Proposals	T. Blank
0.9.5	2008-06-12	Results of Karsruhe 2008-06-04	H. Ziegler
0.9.6	2008-05-12	AES IV, Signature, Ref. SML	U. Pahl
0.9.7	2008-06-14	Clean version and formatting	H. Ziegler / U. Pahl
1.0.0	2008-06-27	Final Version	U. Pahl
1.0.1	2008-07-01	Editorial Revision	U. Pahl
1.0.2	2008-07-21	Some format adaptions; table index added; content index limited to structure level 3.	H. Baden
1.0.3	2009-02-25	Correct mistake in Table 7 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

Table of contents

1 Introduction....6

2 Physical Layer....7

2.1 Twisted Pair Connection (M-Bus)....7

2.1.1 Electrical Specification....7

2.1.2 Hardware Connections and Cable....7

2.2 Wireless Communication (wM-Bus)....7

2.2.1 Modes and Requirements....7

2.2.2 Wireless Data Transmission Intervals....8

2.2.3 Access and Timing of a Meter or Actuator....10

2.2.4 Transmissions Limits and Transmission Credits....11

2.3 Power Line Communication....11

3 Data Link Layer....12

3.1 Wired Communication (M-Bus)....12

3.2 Wireless Communication (wM-Bus)....12

3.2.1 Address-Structure....12

3.2.2 Supported C-Fields....12

3.2.3 Optional Repeater for the Wireless Communication....14

3.2.4 Rules for the MUC....15

4 Application Layer....16

4.1 Overview of Application Layers....16

4.2 Common Part for all Application Layers....17

4.2.1 Supported CI-Fields....17

4.2.2 Access Number....19

4.2.3 Status Byte....20

4.2.4 Supported Device Types (Medium)....21

4.2.5 Encryption....22

4.2.6 Required Values and their Resolution and Accuracy....25

4.3 Generic Services....26

4.3.1 Clock Synchronisation....26

4.3.2 Application Errors after Command....26

5 Application Protocols....27

5.1 M-Bus Application Protocol 27
5.1.1 Supported Data Types (DIF´s) 27
5.1.2 Supported Record Types (VIF's) 27
5.1.3 OBIS-Code 28
5.2 DLMS Application Protocol 28
5.3 SML Application Protocol 28

Annex 29

Annex A (normative): List of OBIS Codes for Basic Meters. 29
Annex B (Normative): OBIS-Declaration via the M-Bus 40
Annex C (Normative): Requirements on the MUC as a Physical M-Bus-Master 41
Annex D (Informative): The Structure of the Application Header 42
Annex E (Normative): Application Error 44
Annex F (Normative): Clock Synchronization 46
Annex G (Informative): Transmission of a Load Profile 47
Annex H (Informative): Gas Meter Consumption Data and their Coding 48
Annex I (Normative): Collision Avoiding Mechanism of the MUC 52
Annex K (Informative): Example of Message Types 57
Annex L (Normative): Timing Diagram 59
Annex M (Informative): Telegram Examples for the M-Bus and the wM-Bus 66
Gas Meter 66
Water Meter 69
Heat Meter 72
Heat Cost Allocator 76
Electricity Meter 79
Installation Procedure with a Special Installation Telegram 88
Send a Command with an Acknowledge 92
Request of the Selected Data 95
Reset of the Link by a SND-NKE 98

List of tables

Table 1: Intervals and reception probability for different applications and different media.....9
Table 2: Accessibility of a meter/actuator.....10
Table 3: C-fields of master (MUC or other communication device).....13
Table 4: C-fields of slave (meter or actuator).....13
Table 5: List of supported CI-fieldsThe application layer standards are: 17
The application layer standards are: 18
Table 6: New device types (Extension of Table 3 in [EN13757-3] (2004)).....21
Table 7: Initialisation vector for the CBC-AES-128 22
Table 8: Contents of meter telegram.....23
Table 9: Contents of MUC authentication 23
Table 10: Definition of the signature word for encryption modes MMMM = 5 or 6.....24
Table 11: Required value resolution with power/flow data.....25
Table 12: Required value resolution without power/flow data.....25
Table 13 – Enumerated values for physical units.....51
Table 14 – Examples for scaler-unit.....51

1 Introduction

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 (MUC or other communication unit). It covers the physical layer, the link layer, the general requirements for encryption and the application itself. They all support alternatively the M-Bus-application-layer, the DLMS/OBIS-application layer and an SML-based application layer. 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).

The references used in this specification can be found in Volume 1 of the Open Metering System Specification (general part).

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

This part concentrates on the requirements for basic meters but also includes some optional enhancements for sophisticated meters. This standard supports both mains powered devices (e.g. electricity meters or actuators) and battery driven devices (e.g. water/gas/heat meters or actuators) with a minimum battery lifetime of up to 14 years.

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 NTA8130.

2 Physical Layer

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

2.1 Twisted Pair Connection (M-Bus)

2.1.1 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 MUC shall be specified by the manufacturer. The minimum requirements are those of a mini master as described in [EN13757-2]. In addition the MUC shall fulfil the requirements of Annex C.

2.1.2 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 100mA (42 V/420 Ω), and reduces the energy converted into heat in the bus interface. For the requirements for wiring and installation refer to [EN13757-2].

2.2 Wireless Communication (wM-Bus)

2.2.1 Modes and Requirements

The [EN13757-4] (2005) 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 user consumption feedback and variable tariffs. The extension to [EN13757-4] 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 [EN13757-5] covering such relaying via meters does not apply to the proposed modes S and T.

As for the various modes described in [EN13757-4], only the modes S1, S2, T1 and T2 are supported by this specification. All these modes operate in various duty-cycle limited sub bands of the 868-870MHz 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.

Note that the total average transmit duty cycle per hour is limited by the [EN13757-4] for the S1-mode to 0.02%, corresponding to a total transmit time of not more than 720ms per hour. The same limit is recommended for all RF communication modes. This is required to limit the collision rate in dense or repeated situations. The CEPT/ERC/REC 70-03 E, see [ERC7003], and the ETSI EN 300220-1 [ETSI-ERM] standards describes further requirements for the physical layer.

S1 and T1 are unidirectional standards where the meter frequently (seconds to hours) transmits telegrams containing meter identification together with metered data. Both modes have been intensively tested and are frequently used in current meter communication systems. This unidirectional function is sufficient to support all required communication functions for a basic meter within the framework of the Open Metering System.

S2 and T2 are compatible bidirectional enhancements of S1 respectively T1. Both enable an optional MUC to meter communication after each meter to MUC telegram. The [EN13757-4] describes all requirements and testing conditions for the four allowed modes T1, T2, S1 and S2. 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 MUC 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 telegram from the MUC as described in [EN13757-4]. 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 1.

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

The proposed signature word in the meter telegram signals to the MUC whether the device can receive data (i.e. implements the S2 or T2 modes), and whether it can receive continuously or only directly after each transmission.

The meter and MUC manufacturers decide which of the four modes are implemented in their products. This requires clear labelling of both, the meter and the MUC as well as the corresponding data sheets so that the customer can choose between interoperable combinations. Note that a MUC might support the communication with one, several or with all four radio communication modes. Please refer to [OMSTC] for the specification of the OMS-MUC.

Note also that the link layer itself does not support multi-telegram messages. Functions requiring more data than the maximum length of a telegram shall handle multi-telegram sequences via the application layer.

2.2.2 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 telegram has to be transmitted at least twice within this maximum update period. Note that according to CEPT/ERC/REC 70-03 E [REC7003] there is a minimum time delay between successive transmissions of 1.8s for the S-modes and 0,72s for the T-Modes.

Therefore a bidirectional meter/actuator (both S- or T-Mode) shall delay every response or acknowledge to the MUC by between min. 2 and max. 5 seconds after reception of the request or command.

See the following table for the mandatory data update periods:

Metering media	Mandatory (billing and actuator)		Informative aspects (consumer)
	Average send interval maximum [min]	Visualization interval for energy provider [h]	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 (submetering)	240.0	24	-
Repeater[1]	240.0	-	-

Table 1: Intervals and reception probability for different applications and different media

Table 1 shows data transmission intervals for informative and billing aspects. For consumers, the visualization data update intervals for different media are 15 respectively 60 minutes at a typical reception probability of more than 95%. Informative intervals are given to provide actual data for consumers.

For billing purposes metering devices have to send their variable meter data at least every 7.5 or 30 or 240 minutes, depending on the media. The individual transmission interval shall vary from ±1% up to ±20% from the average interval. This is required to prevent repeated collisions.

The transmission of installation telegrams (with C=46h) should happen only after a manual installation start event (e.g. push installation button). Installation telegrams shall be transmitted at least 6 times with an interval of 30 to 60 seconds. The transmission of installation telegrams 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 telegram contains fixed data for meter management (like OBIS-Code definitions), it shall be marked as a static telegram (refer to Table 8).

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 telegram (refer to Table 8) and send it at least twice a day.

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

2.2.3 Access and Timing of a Meter or Actuator

A meter/actuator signals its own accessibility in the signature word (encryption mode 0, 5 and 6 only) of every transmission (refer to signature word in Table 10). The meter/actuator initiates periodical transmissions. If the MUC wants to transmit a telegram to a meter dedicated to him it checks in the signature word if the meter is accessible.

Sign. Bit 15 (SigB)	Sign. Bit 14 (SigA)	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)

Table 2: Accessibility of a meter/actuator

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

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

Battery operated bidirectional devices are very restricted in their current consumption. Typically they will provide a short access window only immediately after a transmission. The MUC or other communication device (as master) may initiate a communication to the meter/actuator (as a slave) during this timeslot. The timing conforms to [EN13757-4] and depends on the mode. The referred standard defines for S2-mode a response time of 3 to 50 ms and for T2-mode an acknowledge delay of 2 to 3 ms after transmission.

The response time t_{RO} respective acknowledge delay t_{ACK} (as defined in [EN13757-4]) shall be calculated from the end of the post-amble of meter transmission to the start of the MUC transmission. The transmission of the first chip (bit) of the preamble shall start before the maximum delay of t_{RO} and t_{ACK} expires, and the meter shall then receive the transmission from the MUC or another device correctly.

Note that S1 and S2 modes require a long header as described in [EN13757-4] to facilitate pulsed reception to save receiver current.

If a meter/actuator receives a command or a request it goes into the frequent access cycle. During the frequent access cycle, the meter/actuator will repeat the last message every 2 to 5 seconds until the next request/command is received. This allows the MUC or other communication device to do a fast access sequence to the meter/actuator. The frequent access cycle lasts exactly 30 seconds after the last successful reception of a command or request from the same MUC or another communication device. The MUC can stop the frequent access cycle of the meter/actuator early by sending a SND-NKE-message. The access timing is shown in Annex L.

2.2.4 Transmissions Limits and Transmission Credits

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 MUC 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 additional transmissions. When all transmission credits are used up the meter shall mark this state in the signature word (SigB=0; SigA=1; refer to Table 2) of the last responded telegram and every following spontaneous transmitted telegram as long as no further transmission credits exists. During this period a meter/actuator provides no access to the MUC. The generation of transmission credits is a periodical event. The interval depends on the number of transmission credits per day. A bidirectional meter shall support at least 6 transmission credits per day. Hence a transmission credit shall be generated at least every 4 hours. If a new transmission credit is available, the meter should mark this normal communication state in the signature word of the next transmission (SigB=1).

2.3 Power Line Communication

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

3 Data Link Layer

3.1 Wired Communication (M-Bus)

The link layer is fully described in [EN13757-2]. The selection of a meter by secondary address (refer to [EN13757-3] chapter 11.3) and the support of wild cards for wild card search (refer to [EN13757-3] chapter 11.5) shall be supported. Additionally the support of extended selection method (selection via fabrication number) is also required (refer to [EN13757-3] chapter 11.4). If a meter uses encrypted data transfer then the fabrication number shall be transmitted in the unencrypted area.

The Annex M of this specification contains telegram examples of M-Bus-telegrams.

3.2 Wireless Communication (wM-Bus)

The link layer is fully described in [EN13757-4]. Annex C and D of that standard contain telegram examples together with an application layer according to [EN13757-3] (M-Bus protocol).

3.2.1 Address-Structure

The Address field of the data link layer consist of always the address of the sender. Note that the link layer protocol supports the unique 8 byte device identification consisting of a 2 byte manufacturer identification, the 8 digit (4 byte) BCD coded identification number, an one byte version identification and an one byte device type identification. Additional meter identification schemes like customer number or meter location (e.g. equipment ID) may be implemented via corresponding data records within the application layer.

These four address elements shall be used in the order given in the example of Annex C of [EN13757-4]. Examples are given in Annex M of this specification. Note that for the world-wide uniqueness of the device ID, this 8 byte identification in the data link layer shall be assigned by the manufacturer and must not be changeable by the customer or by the user (e.g. MSO). To assign an additional address if necessary, it has to be applied in the application layer using the long application header (refer to chapter 4.2.1).

3.2.2 Supported C-Fields

The C-field is used to declare the message types. It is conform to the unbalanced C-fields of [EN60870-5-2].

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
- Special messages for installation

The message dialog type is signalled by the C-field. The following C-fields may be generated by the master (MUC or other communication device) and shall be accepted by the slave (meter/actuator).

Message types of master	**C-fields (hex)**	**Explanation**	**Required response of bidirectional slave**
SND-NKE	40h	Link reset after communication; Also signals capability of reception of a meter/ actuator after reception of installation telegrams	
SND-UD	53h[2], 73h	Send command (Send User Data)	ACK
REQ-UD1	5Ah, 7Ah	Alarm request , (Request User Data Class1)	ACK, RSP_UD
REQ-UD2	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 MUC	-

Table 3: C-fields of master (MUC or other communication device)

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

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

Message types of slaves	**C-fields (hex)**	**Explanation**	**Required response of master**
SND-NR	44h	Send spontaneous/periodical application data without request (Send /No Reply)	-
SND-IR	46h	Send manually initiated installation data; (Send Installation Request)	CNF-IR
ACC-DMD	48h	Access demand to master in order to request new important application data (alerts)	ACK
ACK	00h, 10h, 20h, 30h	Acknowledge the reception of a SND-UD or SND-NKE (acknowledgement of transmission only); It shall also be used as a response to an REQ-UD1, when no alert happened	-
RSP-UD	08h, 18h, 28h, 38h	Response of application data after a request from master (response of user data)	-

Table 4: C-fields of slave (meter or actuator)

[2] The use of bits FCB, FCV, ACD and DFC shall conform to [EN 60870-5-2]!

Only message types RSP-UD and SND-NR can be applied to transport application data from a meter/actuator. 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.

For unidirectional transmitting basic meters with modes S1 or T1, the support of C-field values 44h and optionally 46h (for support of tool-less installation mode for MUC without external installation support) is required. For all message types with application data (SND-UD; RSP-UD, SND-NR, SND-IR) the identical link layer and the identical fixed application layer header as described in the [EN13757-4] are used for all application layers. The structure of this application header and the following application layer is defined by the CI-field. For all other message types without application data the application header conforms to the new applied CI-field for data link extension (refer to Annex D).

The slave has to reply to every message with an expected response of the master, independently of whether this message was already received earlier (refer to chapter 4.2.2). Exceptions to this rule are described in chapter 2.2.3. The timing and interaction between different message types are shown in Annex L.

3.2.3 Optional Repeater for the Wireless Communication

If a direct wireless transmission between a meter/actuator and a MUC 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 telegrams 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 1). It may optionally send installation telegrams (with C=46h) within given time limits (refer to chapter 2.2.2).

A repeater may be a dedicated device or a function integrated into a meter or a MUC. An integrated repeater should use the address of the hosted meter or the MUC. Both integrated and dedicated repeaters should always apply the device type “repeater” (refer to Table 6) to transmit the repeater management data.

It will be distinguished between:

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

3.2.3.1 Unidirectional Repeater

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

The hop counter bits are not supported for encryption mode 4 or less. Therefore a repeater should repeat telegrams with an encryption mode 5, 6, or 0 only. All other telegrams shall be ignored.

It just retransmits (with some delay) a received Open Metering System compatible telegram with a hop counter = 0 only. The hop counter is placed in the signature word (see chapter 4.2.5.4). The repeater has to increment the hop counter to 1 before retransmission, what requires the recalculation of the CRC value for the second block. The use of hop counter value 2 or 3 is reserved for future options.

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 telegrams. Also the transfer of the meter time will not be accurate.

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 telegram (with C= 46h) with a hop counter = 0 it shall 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 telegram. 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.

3.2.3.2 Bidirectional Repeater

[WORKITEM] A fully functional bidirectional repeater will be defined in a later revision of this specification.

3.2.4 Rules for the MUC

If the MUC receives an installation telegram 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 telegram. In addition it may generate a CNF_IR telegram to the meter to signal its assignment to this MUC.

In case of an erroneous multiple assignment of one meter/actuator to several MUC's, collisions may happen when more than one MUC access a meter/actuator. To solve this failure every MUC 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 MUC shall provide a clock synchronisation service (refer to chapter 4.3.1).

4 Application Layer

4.1 Overview of Application Layers

The application layer has always a fixed frame structure as described in [EN13757-3]. It may transport either the meter application layer according to [EN13757-3] (M-Bus), or alternatively [EN13757-1] (COSEM/DLMS/SML-type communication primarily used by electricity meters). Note that the CI field as the first byte of the application layer distinguishes between these application layer protocol types and frame structures. A MUC or a user 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 telegrams. This specification part covers mainly the M-Bus variant. Note that the MUC or the display shall be able to parse any legal (M-Bus or COSEM/DLMS/SML) application layer telegram into separate data points. But it is sufficient to “understand” i.e. decode only the required values stated below.

4.2 Common Part for all Application Layers

4.2.1 Supported CI-Fields

The frame format of the application layer is the same for all application protocols. It consists of a common header that ends with a CI-byte, which indicates the main telegram function and the type of coding (i.e. the application protocol) used for the rest of the telegram. The following CI-fields shall be supported:

CI-field	Direction	Header length	Application protocol
50h	Application select to device	None	M-Bus
51h	CMD to device	None	M-Bus (for wired M-Bus only!)
52h	Selection of device	None	M-Bus
5Ah	CMD to device	4 Bytes	M-Bus +
5Bh	CMD to device	12 Bytes	M-Bus +
60h	CMD to device	14 Bytes	DLMS+
61h	CMD to device	6 Bytes	DLMS+
64h	CMD to device	14 Bytes	SML+
65h	CMD to device	6 Bytes	SML+
6Ch	Time Sync	14 Byte	Generic
6Dh	Time Sync	14 Byte	Generic
70h	Error from device	None	Generic
71h	Alarm from device	None	Generic
72h	Response from device	12 Bytes	M-Bus
78h	Response from device	None	M-Bus (not used for OMS
7Ah	Response from device	4 Bytes	M-Bus
7Ch	Response from device	14 Bytes	DLMS+
7Dh	Response from device	6 Bytes	DLMS+
7Eh	Response from device	14 Bytes	SML+
7Fh	Response from device	6 Bytes	SML+
80h	Link extension to device	12 Byte	none+
8Ah	Link extension from device	4 Bytes	none+
8Bh	Link extension from device	12 Bytes	none+

Table 5: List of supported CI-fields

The application layer standards are:

- M-Bus: [EN13757-3]
- M-Bus+: Planned future revision of the [EN13757-3] (CI-values reserved so far)
- DLMS/SML+, [EN13757-1], [DLMS-UA] or [SML-spec]: Planned future revision of the [EN13757-3].

The header structures are:

- 4 bytes: As for CI=7Ah of [EN13757-3],
  If the telegram contains such a “short” header the meter identification is taken from the link layer,
- 12 bytes: As for CI=72h of [EN13757-3],
  If the telegram contains such a “long” header, this header contains (independent of transmission direction) always the meter/actuator identification.

Note that with a 12-byte header the device (meter/actuator) address is contained in this header, whereas the manufacturer assigned unique link layer address may be different (but still within the common universally unique address structure). This allows, for example a wired to wireless converter, to supply the supported meter address in the 12-byte header and its own address in the link layer. For a simple meter or actuator (which doesn’t need an additional converter) the shorter 4-byte header is sufficient.

The short and the long header of the SML and DLMS application protocols are additionally extended by a 2 byte encryption test sequence (refer to 4.2.5.5). In the M-Bus application protocol the encryption test sequence is a part of the application data.

Every application header for wM-Bus has to contain at least:

- Access number
- Status byte
- Signature word

4.2.2 Access Number

4.2.2.1 Access Number for wM-Bus

The access number together with the transmitter address is used to identify a telegram. When a received telegram contains a new access number it consists of new data. But if the same access number was received previously from this sender, the content of the telegram is also the same.

It will be distinguished between:

- Meter access number
- MUC access number

The meter access number is generated by a meter/actuator. It will be incremented by 1 (and only 1) for every new transmission. When periodical data telegrams are generated a new access number shall always be applied even if the consumption value has not changed (to avoid replay attack!). For the repetition of the last transmitted telegram (e.g. last installation telegram) the last (old) access number should also be used. The meter access number shall be applied to SND-NR, SNR-IR and ACK-DMD telegrams. If a MUC accepts an ACK-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 MUC access number has no impact on the stored meter access number of the meter/actuator.

The MUC access number is generated by the MUC. It may be selected without any restrictions. However the MUC shall not use the same access number for a new telegram to the same meter/actuator again within 300 seconds.

The meter/actuator shall not expect any specific order of access numbers in telegrams received from the MUC. It shall only distinguish between a new and an old telegram. The last received access number marks an old telegram. 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 2.2.3) it shall clear the last received MUC 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, REQ-UD1 or REQ-UD2, it shall use the received MUC access number for its response or acknowledgement. The MUC may recognize an outstanding response or acknowledgement by its own access number. Hence the meter/actuator repeats the last response or acknowledgement, if the MUC sent the request or the command with the old access number again. Otherwise it shall generate a new telegram with the new access number received from the MUC.

4.2.2.2 Access Number for M-Bus

For wired M-Bus the Access number shall be conform to the [EN13757-3].

4.2.3 Status Byte

It will be distinguished between:

- MUC status (applied with CI-field 5Ah, 5Bh, 60h, 61h, 64h, 65h, 6Ch, 6Dh or 80h)
- Meter status (applied with CI-field 72h, 7Ah, 7Ch, 7Fh, 8Ah or 8Bh)

4.2.3.1 MUC-Status

The MUC status field contains information about the reception level of the meter/actuator transmission. It is coded as follows:

Bit #	Value
0 ... 5	Received RSSI value for a reception level in range of -128 ... -6dbm Reception level is calculated by -130dbm+2 * RSSI-Value (1 ... 62) If RSSI value = 0 no reception level is available If RSSI value = 63 the reception level is > -6dbm
6	Reserved (0 by default)
7	Reserved (0 by default)

Information about link quality is helpful for the rating of several radio links between a meter/actuator and different MUCs. It will be also used for signalling the link quality to an installation service tool. Therefore the MUC should support a valid RSSI-value.

4.2.3.2 Meter Status

The Meter status byte shall conform to [EN13757-3] (2004). The bit “any application error” (refer to table 5 of [EN13757-3] (2004)) signals an error during execution of the last received command. A detailed application error (with CI=70h) will be returned at the next request (REQ_UD2). The codes for application errors are listed in table 14 of [EN13757-3] (2004).

An extension of this error codes for OMS is listed in Annex E.

4.2.4 Supported Device Types (Medium)

For the Open Metering System the meter device types 02h (electricity), 03h (gas), 04h (heat), 06h (warm water) 07h (water) 08h (heat cost allocator), 0Ah and 0Bh (cooling load meters inlet/outlet), 0Ch (heat - measured at inlet), 0Dh (heat/cooling load), and actuator 21h (valve) shall be supported at minimum.

Additionally the system devices 25h (display), 31h (MUC) and 32h (unidirectional repeater) shall be supported. (Note that a bidirectional repeater (33h) is defined and will be specified in a future revision.)

Table 3 of device types in [EN13757-3] (2004) has to be expanded for new devices.

Device Type (	**Binary (Bit 7..0)**	**Hex**
Display device	0010 0101b	25h
OMS MUC	0011 0001b	31h
OMS unidirectional repeater	0011 0010b	32h
OMS bidirectional repeater	0011 0011b	33h
Reserved for Smart Metering Electricity Meter[3]	0100 0010b	42h
Reserved for Smart Metering Gas Meter	0100 0011b	43h
Reserved for Smart Metering Heat Meter	0100 0100b	44h
Reserved for Smart Metering Water Meter	0100 0111b	47h
Reserved for Smart Metering Heat Cost Allocator	0100 1000b	48h

Table 6: New device types (Extension of Table 3 in [EN13757-3] (2004))

[3] These device types are reserved for a future standardised Smart Meter. Meters applying this OMS-Specification shall use device types according to [EN13757-3] (2004)

4.2.5 Encryption

4.2.5.1 General Structure

In order to support data privacy and to prevent zero consumption detection, encryption is required for wireless communication. All metered consumption values (i.e. both actual values and stored values) shall be encrypted. In addition, the optional flow, power or temperature values shall be encrypted. For wired communication encryption of meter data is optional.

The link layer header (including ID) and the fixed 4-byte or 12-byte application header after the CI-field, are never encrypted. The encryption mode does not use the obsolete DES modes 2 or 3 as suggested in [EN13757-3] (2004). Instead, the AES-encryption with a block size of 16 Bytes and a 128 Bit key with cipher block chaining are required. The CBC (Cipher Block Chaining) encryption for AES128 uses a 128 bit (16 Byte) initialisation vector to start the encryption of the first block. In this specification two types of initialisation vectors will be supported. This results in different encryption modes as declared in the signature word (referred to as encryption methods in [EN13757-3] (2004)):

- Encryption mode 4 (static initialisation vector, to be conform with NTA 8130, not recommended for new developments)
- Encryption mode 5 (dynamic initialisation vector, mandatory for OMS)
- Encryption mode 6 (so far reserved, refer to Table 10)
- Encryption modes 7 to 15 (for future purposes)

4.2.5.2 Initialisation Vector for Encryption Mode 4

Refer to NTA 8130 P2-Companion standard.

4.2.5.3 Initialisation Vector for Encryption Mode 5

The initialisation vector for encryption mode 5 is (written in low to high order according to the AES standard FIPS 197):

LSB	1	2	3	4	5	6[4]	7	8	9	10	11	12	13	14	MSB
Manuf. (LSB)	Manuf. (MSB)	ID (LSB)	..	..	ID (MSB)	Ver-sion	Med-ium	Acc. no.	..	..	..	..	..	..	Acc. no.

Table 7: Initialisation vector for the CBC-AES-128

To make sure that the encrypted and the unencrypted section of the telegram came from the same meter, this initialisation vector contains in its lower 8 bytes the meter identification (from link or application layer, depending on the CI-field (refer to chapter 4.2.1)).

When the consumption value does not change, this could be detected by reception of periodical telegrams from the meter. To protect the consumer from unauthorised observation of such a situation with zero consumption, each generated telegram shall change with every periodical transmission. This can be implemented either by a timestamp in the first block or by an increased access number (Acc. no.), which is part of the initialisation vector (copy 8 times the access number to the upper 8 bytes). Due to the block chaining mode CBC both methods will influence all other encrypted blocks.

[4] Note that in the earlier version V1.0.2 of [OMSPC] Vol.2,
version and medium of the initialisation vector was described in the wrong order!

4.2.5.4 Signature Word (Encryption Mode and Communication Status Bits)

The signature word in general declares the length and method of data encryption. For encryption mode 5 and 6 additional communication status bits are defined. The meaning of these special bits differs between encryption mode 5 and 6, and lower modes. Only the bits "MMMM" and "NNNN" are supported in lower encryption modes (refer to Table 10). For the communication on wired M-Bus all bits in the signature word except "MMMM" and "NNNN" should be set to "0".

The coding of the signature field for the AES encryption mode with a dynamic initialisation vector is 5 (so far reserved) (MMMM=0101b). The high nibble "NNNN" of the lower byte declares the number of encrypted 16 byte blocks, and the low nibble Bit0 and Bit1 (HH) are used as a hop counter in repeated telegrams. For a meter or actuator they are always zero. Bit2 and Bit3 (CC) are used to describe the contents of the telegram.

Sig. Bit 3	Sig. Bit 2	Contents of the telegram
0	0	Standard data telegram with unsigned variable meter data (conform to OMS-Vol2 V1.02).
0	1	Signed data telegram (consists of meter data with a signature approved for billing).
1	0	Static telegram (consists of parameter, OBIS-definitions and other data points which are not frequently changed). Static telegrams shall be transmitted at least twice a day.
1	1	Reserved for future extensions.

Table 8: Contents of meter telegram

Sig. Bit 3	Sig. Bit 2	Contents of data point authentication.
0	0	Standard command telegram.
0	1	Reserved for authenticated command telegram type 1.
1	0	Reserved for authenticated command telegram type 2.
1	1	Reserved for future extensions.

Table 9: Contents of MUC authentication

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

The signature bits A and B are used for access control to the meter /actuator as described in chapter 2.2.3. Thus, the complete signature word is:

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	reserved	reserved	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 telegram	content of telegram	hop counter	hop counter
B	A	0	0	M	M	M	M	N	N	N	N	C	C	H	H

Table 10: Definition of the signature word for encryption modes MMMM = 5 or 6

Partial encryption may be used to allow unencrypted access to operational parameters. The encrypted bytes follow as one or several encrypted 16 byte blocks directly after the header. Optional unencrypted bytes may follow the encrypted blocks if the link layer telegram length signals more bytes than the encryption length of 16*NNNNb bytes in the low byte of the signature word. At least 8 bytes of the encryption key shall be different for each meter.

The full 16 byte key shall be assigned by the manufacturer together with the meter identification and safely transferred to its customers. The format is according to [FIPS197].

4.2.5.5 Decryption Verification

In order to verify that the telegram is decrypted correctly, the encrypted part shall start with a known sequence. For encryption mode 4 it is required to start with a data point containing “date and time”. A device supporting encryption mode 5 shall start with two bytes of 2Fh (=idle filler DIF) before the first data record. Since the telegram must have an encrypted length of an integer multiple of 16 bytes, such idle filler bytes often would also be added at the end of the last encrypted block. Note if encryption mode 5 is used on wired M-Bus then the two byte idle filler 2Fh 2Fh shall be applied after the signature word as well. For the application header of SML or DLMS these 2 bytes are a part of the application header.

4.2.5.6 Examples

Annex M shows examples with both unencrypted and encrypted data.

4.2.6 Required Values and their Resolution and Accuracy

For the Open Metering System each telegram for billing purposes shall at least contain the actual metered value with the meter accuracy and sufficient resolution for billing. Each telegram for consumer information shall contain sufficient information and accuracy to enable the MUC to display power respectively flow with sufficient accuracy and resolution. This can either be implemented via extra data points for flow respectively power or by sufficient resolution of the meter index and sufficient information about the time between indexed values. Unified telegrams for both purposes may be used if both requirements are met.

4.2.6.1 Required Resolution if an extra Data Point for Flow (respectively Power) is Transmitted.

The required value resolutions in this case are:

Medium	Billing	Power/flow resolution
Electricity	<= 1kWh	<= 1W
Water	<= 1m³	No requirement
Gas QMax <=6 m³/h	<= 1m³	<= 10l/h
Gas QMax <=60 m³/h	<= 1m³	<= 100l/h
Gas QMax > 60 m³/h	<= 1m³	<= 1000l/h
Heat / Cold Qp < 10m³/h	<= 1kWh	No requirement
Heat / Cold Qp < 100m³/h	<= 10kWh	No requirement
Heat / Cold Qp >= 100m³/h	<= 100kWh	No requirement
Heat cost allocation	No requirement	No requirement

Table 11: Required value resolution with power/flow data

The power/flow values shall be averaged either over the average transmission period length or the averaging duration shall be transmitted in an extra data point.

4.2.6.2 Required Resolution if no extra Data Point for Flow (respectively Power) is Transmitted.

If the meter transmits only index values the MUC must be able to calculate the flow respectively power with sufficient resolution and accuracy from the index value and the time interval between the index values. This requires the following index resolutions.

Medium	Index resolution
Electricity	<= 0.1 Wh
Water	<= 1m³
Gas QMax <=6 m³/h	<= 10 l
Gas QMax <=60 m³/h	<= 100 l
Gas QMax > 60 m³/h	<= 1000 l
Heat / Cold	No requirement
Heat cost allocation	No requirement

Table 12: Required value resolution without power/flow data

4.2.6.3 Required Time Information

In addition, if there is no power/flow information present there are requirements for the accuracy and resolution of the actual time difference between the index values to ensure a time interval accuracy and resolution of <= 1%. These requirements can be fulfilled by one of the following alternatives.

4.2.6.3.1 Correlated Transmission

If the meter spontaneously transmits the index value with a fixed delay of less than half the transmission interval and if such a delay varies by less than 1% of the transmission interval then the MUC can calculate the index time difference from the telegram arrival times with sufficient resolution and accuracy.

4.2.6.3.2 Uncorrelated Transmission

If the difference of delays of transmission time points varies by more than 1% of the transmission interval, each telegram shall contain sufficient time information to calculate this time difference. This can either be implemented with a (date)/time data point with a resolution of 1s in each telegram or with a data point signalling the actual time delay between index time and transmit time with a resolution of 1 s.

4.2.6.3.3 Transmission on Request

If the meter transmits the index value due to a request it has to refer to the time of the value generation at the moment of the first transmission of the request (REQ_UD2) by the MUC or another communication unit. The meter/actuator may generate the response with a fixed delay, which should not vary by more than 1 second. A potential runtime of the request from the MUC to the meter/actuator shall be considered. Hence a unique reference time is given even when the response is repeated several times.

4.3 Generic Services

4.3.1 Clock Synchronisation

The MUC shall provide the correct time (UTC) for every bidirectional meter/actuator both periodically and on event. In the following cases a clock synchronisation shall be applied:

- Once every day (as long as the MUC has a valid time)
- When the MUC 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 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 Annex F describes the transmission of clock synchronisation to meter/actuator.

4.3.2 Application Errors after Command

When a meter/actuator detects a failure during the interpretation or the execution of a received command it shall generate an application error. The application error may be requested by the MUC with a REQ-UD2 as long as the frequent access cycle is still active (refer to chapter 2.2.3). 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 frame CI=70h as defined in [EN13757-3] (2004).

5 Application Protocols

5.1 M-Bus Application Protocol

5.1.1 Supported Data Types (DIF´s)

For the metered values only the data types A or B (BCD-integer or binary fixed length) as defined in Annex A and Annex B of [EN13757-3] (2004) are allowed. For all other required values the data field values of 0101b (floating point) are not allowed. For the variable length data type (1101b) the LVAR (data length) values of 00h to 0BFh (up to 192 characters of ASCII string) and 0E0h to 0EFh (variable length binary) is allowed. To be able to accommodate signatures with more than 120 bits (15 bytes) length the LVAR definition for variable length binary numbers (0E0h … 0EFh) of the current standard is extended to (0E0h ... 0F7h), thus allowing binary numbers of up to 23 bytes (184 bits). The new defined codes (0F0h ... 0F7h) had been reserved so far.

The data field values 0XFh are also allowed. In the DIF or DIFE nonzero values for subunit, storage number or tariff are allowed, but are limited to a maximum value of 255.

For records with date and/or time data the data types F, G, I and J defined in Annex A of [EN13757-3] (2004) shall be supported.

5.1.2 Supported Record Types (VIF's)

Measured values and units

The required values shall be coded for the compulsory (electrical) energy with one of the VIFs E0000nnnb (1mWh to 10 kWh) or VIF= 0FBh with VIF-extension E000000nb (0.1MWh to 1MWh). If required because of insufficient resolution of the metered values, the (electrical) power shall use the VIFs E0101nnnb (1mW to 10 kW) or VIF=0FBh with VIF-extension E010100nb (0.1MW to 1 MW).

For thermal energy the GJ unit-VIFs E0001nnnb (1J to 10MJ) or E000100nb (0.1 GJ to 1 GJ) are additionally allowed.

For the required volume the VIFs E0010nnnb (1ml to 10 m^3) shall be used, whereas for the possibly required flow the VIFs E0111nnnb (1ml/h to 10m^3/h) are allowed.

For H.C.A. (heat cost allocator) units the primary VIF E110 1110 shall be used.

For the optional temperature E10110nnb (flow temp. 1m°C to 1°C), E10111nnb (return temperature) or E11000nnb for temperature difference (1mK to 1K) shall be used,

All these values may use the VIF=0FBh with the (combinable/orthogonal) VIF-extensions E1110nnn (Factor of 0.000001 to 10) as an additional decimal power scaling.

For the gas meter it will distinguished between volume at measurement condition, temperature converted volume and volume at base condition. The orthogonal VIFE E0111010b shall be used to declare the volume at measurement conditions, and the orthogonal VIFE E0111110b shall be used to declare the volume at base conditions. A volume with no VIF-Extension declares the temperature converted volume. Details are described in Annex H.

Date, time and intervals

For optional date and/or time the VIFs E1101100b or E1101101b (with data fields 0100b, 0011b or 0110b) shall be used. Note that the MUC sends date and time in all command telegrams, to ensure that the meter/actuator can detect a replay of an old MUC-command.

The meter/actuator shall not use this time stamp for synchronisation of its clock. There is a generic service (CI=6Ch, 6Dh) used for synchronisation of meter/actuator clock.

For an uncorrelated transmission the optional time between measurement and transmission (run time) shall be coded as E11101nnb (1s to 1day).

For the averaging time interval of power or flow values E11100nnb (averaging duration) shall be used.

Management data

For optional transmission of ownership number the VIF=0FDh with VIF-extension E0010001 (customer) shall be used, the content of the ownership number remains user specific.

For optional transmission of the metering point identifier (Location ID) the VIF=0FDh with VIF-extension E0010000 (customer location) shall be used.

For meter management it may be useful to add the reception level of a received radio device. The reception level should use VIF=0FDh with VIF extension E1110001 (so far reserved). The value is given in dBm.
Example: 01 FD 71 A1 means -95 dBm (binary) and 0A FD 71 85 F0 means -85 dbm (BCD). If no value available the value should be set invalid like 01 FD 71 80 (binary).

This VIFE may also be used together with the Function field 10b in DIF to declare preset quality limit of the reception level which was exceeded by the received radio device. Example: 21 FD 71 9C marks a reception level > -100 dBm.

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

Else

All other VIFs and DIFs of [EN13757-3] are allowed, but here decoding by the MUC or display is optional and not required.

5.1.3 OBIS-Code

M-Bus coded metering data needs a relation to a relevant OBIS-code. The table in Annex A lists a subset of M-Bus-data points and the assigned OBIS-codes. A MUC which is converting M-Bus data points to another application protocol shall add an OBIS-code to every M-Bus data point according to Annex A.

If a meter/actuator uses an M-Bus data point which is not listed in Annex A and which is required for billing purposes then the OBIS-declaration should be transmitted from the meter/actuator itself. A radio device should transmit this OBIS-declaration by a static telegram (refer to Table 8). The MUC then adds this OBIS-declaration to the default OBIS-conversion-table. The OBIS-declaration via the M-Bus application protocol is described in Annex B.

5.2 DLMS Application Protocol

The DLMS application protocol for CEN meters is described in [EN13757-1].

5.3 SML Application Protocol

The SML application protocol is described in document [SML-spec]. An example based on “SML - Smart Message Language” Version 1.03 is listed in Annex M (Electricity meter).

Annex

Annex A (normative): List of OBIS Codes for Basic Meters.

This list describes the relation of OBIS-code to a received M-Bus record.

M	Mandatory (These data objects have to be specified)
Ax	Alternatively (One of the with 'A' and identical number marked data objects are mandatory)
O	Optional (These data objects do not need to exist)

Bit symbol	Note
ssss ssss	Status byte, according to table 4 of EN 13757-3 (2204)
cccc	Coding of the data field, according to table 6 of EN 13757-3(2004) (except real, variable length, selection for readout, special functions)
n	One or more Bits, according to tables 9, 11, 12, 13 of EN 13757-3(2004)
VZ	Recent value 1 ≤ VZ ≤ 99 or 101 ≤ VZ ≤ 124
x	Definition of the Bit of the M-Bus storage number, which is equivalent to the billing period counter (VZ) (see EN 13757-3(2004), figures 6 and 7); value range 0 … 99 and 101 ..124

Note that the B-Field of the OBIS Code shall be build from the subunit in related DIFE of data point (refer to EN13757-3 (2004) chapter 6.10).
If the meter uses one channel only then the subunit and also the B-Field of the OBIS -Code shall be 0 (as listed in this table).
If a meter uses more than one channel then the subunit and also B-Field of OBIS-Code shall be declare channel number which starts with 1.

5

	Type	OBIS-Code	Description	DIF/DIFE or fixed fields	VIF/VIFE
	Abstract	**0**	**All**		
M	Error status	0-0:97.97.0*255	Status according to EN13757-3		
	–		*Status*	ssss ssss	
M	Current time	0-0:0.9.1*255	Local time (Receiving time of MUC)		
	–		*Data object generated automatically by MUC!*		
M	Current date	0-0:0.9.2*255	Local date (Receiving date of MUC)		
	–		*Data object generated automatically by MUC!*		
M	Device address	0-0:96.1.1*255	Device address (assigned by the manufacturer)		
	–		*complete device address (manufacturer, meter ID,version, device type)*		
O	Ownership number	0-0:96.1.9*255	Ownership number (optional)		
	–		*Fixed length*	0000 cccc	1111 1101 0001 0001
	–		*Variable length*	0000 1101	1111 1101 0001 0001
O	Metering point ID	0-0:96.1.10*255	Identification of the metering point		
	–		*Fixed length*	0000 cccc	1111 1101 0001 0000
	–		*Variable length*	0000 1101	1111 1101 0001 0000
O	Serial number	0-0:96.1.0*255	Serial number (assigned by the manufacturer)		
	–		*Fixed length*	0000 1100	0111 1000

	Electricity	**1**	**02_h**								
A1	Meter count	1-0:1.8.0*255	Active energy import (+*A*), current value								
	–	kWh	10e-6 … 10e+1	0000 cccc			0000 0nnn				
	–	kWh	10e+2 … 10e+3	0000 cccc			1111 1011	0000 000n			
	–	kWh	10e+5 … 10e+6	0000 cccc			1111 1011	1000 000n	0111 1101		
O	Meter count	1-0:1.8.0*VZ	Active energy import (+*A*), recent value								
	–	kWh	10e-6 … 10e+1	1x00 cccc	1000 xxxx	0000 00xx	0000 0nnn				
	–	kWh	10e+2 … 10e+3	1x00 cccc	1000 xxxx	0000 00xx	1111 1011	0000 000n			
	–	kWh	10e+5 … 10e+6	1x00 cccc	1000 xxxx	0000 00xx	1111 1011	1000 000n	0111 1101		
A1	Meter count	1-0:2.8.0*255	Active energy export (-*A*), current value								
	–	kWh	10e-6 … 10e+1	0000 cccc			1000 0nnn	0011 1100			
	–	kWh	10e+2 … 10e+3	0000 cccc			1111 1011	1000 000n	0011 1100		
	–	kWh	10e+5 … 10e+6	0000 cccc			1111 1011	1000 000n	1111 1101	0011 1100	
O	Meter count	1-0:2.8.0*VZ	Active energy export (-*A*), recent value								
	–	kWh	10e-6 … 10e+1	1x00 cccc	1000 xxxx	0000 00xx	1000 0nnn	0011 1100			
	–	kWh	10e+2 … 10e+3	1x00 cccc	1000 xxxx	0000 00xx	1111 1011	1000 000n	0011 1100		
	–	kWh	10e+5 … 10e+6	1x00 cccc	1000 xxxx	0000 00xx	1111 1011	1000 000n	1111 1101	0011 1100	
O	Time of count	1-0:0.9.1*255	Current time at time of transmission								
	–	Type F		0000 0100			0110 1101				
O	Date of count	1-0:0.9.2*255	Current date at time of transmission								
	–	Type G		0000 0010			0110 1100				
	–	Type F		0000 0100			0110 1101				
O	Date of count	1-0:0.1.2*VZ	Local date at time of recent meter value								
	–	Type G		1x00 0010	1000 xxxx	0000 00xx	0110 1100				
	–	Type F		1x00 0100	1000 xxxx	0000 00xx	0110 1101				
O	Time integral	1-0:0.8.2*255	Averaging duration for actual power value								
	–	h *or* min *or* sec		0000 cccc			0111 00nn				

	HCA	**4**	**08_h**		
M	Meter count	4-0:1.0.0*255	Unrated integral, current value		
	–	HCA	10e+0	0000 cccc	0110 1110
M	Meter count	4-0:1.2.0*255	Unrated integral, set date value		
	–	HCA	10e+0	0100 cccc	0110 1110
O	Time of count	4-0:0.9.1*255	Current time at time of transmission		
	–	Type F		0000 0100	0110 1101
O	Date of count	4-0:0.9.2*255	Current date at time of transmission		
	–	Type G		0000 0010	0110 1100
	–	Type F		0000 0100	0110 1101
M	Date of count	4-0:0.1.10*255	Local date at set date	(target date)	
	–	Type G		0100 0010	0110 1100

	Cooling	**5**	**0A$_h$, 0B$_h$**	**(Cooling only)**				
M	Meter count	5-0:1.0.0*255	Energy (*A*), total, current value					
	–	kWh	10e-6 ... 10e+1	0000 cccc	0000 0nnn			
	–	kWh	10e+2 ... 10e+3	0000 cccc	1111 1011	0000 000n		
	–	kWh	10e+5 ... 10e+6	0000 cccc	1111 1011	1000 000n	0111 1101	
	–	GJ	10e-9 ... 10e-2	0000 cccc	0000 1nnn			
	–	GJ	10e-1 ... 10e+0	0000 cccc	1111 1011	0000 100n		
	–	GJ	10e+2 ... 10e+3	0000 cccc	1111 1011	1000 100n	0111 1101	
O	Meter count	5-0:1.2.0*255	Energy (*A*), total, set date value					
	–	kWh	10e-6 ... 10e+1	0100 cccc	0000 0nnn			
	–	kWh	10e+2 ... 10e+3	0100 cccc	1111 1011	0000 000n		
	–	kWh	10e+5 ... 10e+6	0100 cccc	1111 1011	1000 000n	0111 1101	
	–	GJ	10e-9 ... 10e-2	0100 cccc	0000 1nnn			
	–	GJ	10e-1 ... 10e+0	0100 cccc	1111 1011	0000 100n		
	–	GJ	10e+2 ... 10e+3	0100 cccc	1111 1011	1000 100n	0111 1101	
O	Power	5-0:8.0.0*255	Power (energy flow) (*P*), average, current value					
	–	W	10e-3 ... 10e+4	0000 cccc	0010 1nnn			
	–	kJ/h	10e-3 ... 10e+4	0000 cccc	0011 0nnn			
O	Flow rate	5-0:9.0.0*255	Flow rate, average (V_a/t), current value					
	–	m³/h	10e-6 ... 10e+1	0000 cccc	0011 1nnn			
O	Time of count	5-0:0.9.1*255	Current time at time of transmission					
	–	Type F		0000 0100	0110 1101			
O	Date of count	5-0:0.9.2*255	Current date at time of transmission					
	–	Type G		0000 0010	0110 1100			
	–	Type F		0000 0100	0110 1101			
O	Date of count	5-0:0.1.10*255	Local date at set date					
	–	Type G		0100 0010	0110 1100			
O	Time integral	5-0:0.8.5*255	Averaging duration for actual power value					
	–	h *or* min *or* sec		0000 cccc	0111 00nn			

	Cooling	**5**	**0D$_h$ (cooling)**	**(Combined heat/cooling)**					
M	Meter count	5-0:1.0.0*255	Energy (*A*), total, current value						
	–	kWh	10e-6 … 10e+1	1000 cccc	0001 0000	0000 0nnn			
	–	kWh	10e+2 … 10e+3	1000 cccc	0001 0000	1111 1011	0000 000n		
	–	kWh	10e+5 … 10e+6	1000 cccc	0001 0000	1111 1011	1000 000n	0111 1101	
	–	GJ	10e-9 … 10e-2	1000 cccc	0001 0000	0000 1nnn			
	–	GJ	10e-1 … 10e+0	1000 cccc	0001 0000	1111 1011	0000 100n		
	–	GJ	10e+2 … 10e+3	1000 cccc	0001 0000	1111 1011	1000 100n	0111 1101	
O	Meter count	5-0:1.2.0*255	Energy (*A*), total, set date value						
	–	kWh	10e-6 … 10e+1	1100 cccc	0001 0000	0000 0nnn			
	–	kWh	10e-6 … 10e+1	1100 cccc	0000 0000	1000 0nnn	0011 1100		
	–	kWh	10e+2 … 10e+3	1100 cccc	0001 0000	1111 1011	0000 000n		
	–	kWh	10e+5 … 10e+6	1100 cccc	0001 0000	1111 1011	1000 000n	0111 1101	
	–	GJ	10e-9 … 10e-2	1100 cccc	0001 0000	0000 1nnn			
	–	GJ	10e-9 … 10e-2	1100 cccc	0000 0000	1000 1nnn	0011 1100		
	–	GJ	10e-1 … 10e+0	1100 cccc	0001 0000	1111 1011	0000 100n		
	–	GJ	10e+2 … 10e+3	1100 cccc	0001 0000	1111 1011	1000 100n	0111 1101	
O	Power	5-0:8.0.0*255	Power (energy flow) (*P*), average, current value						
	–	W	10e-3 … 10e+4	1000 cccc	0001 0000	0010 1nnn			
	–	kJ/h	10e-3 … 10e+4	1000 cccc	0001 0000	0011 0nnn			
O	Flow rate	5-0:9.0.0*255	Flow rate, average (V_a/t), current value						
	–	m³/h	10e-6 … 10e+1	1000 cccc	0001 0000	0011 1nnn			
O	Time of count	5-0:0.9.1*255	Current time at time of transmission						
	–	Type F		1000 0100	0001 0000	0110 1101			
O	Date of count	5-0:0.9.2*255	Current date at time of transmission						
	–	Type G		1000 0010	0001 0000	0110 1100			
	–	Type F		1000 0100	0001 0000	0110 1101			
O	Date of count	5-0:0.1.10*255	Local date at set date						
	–	Type G		1100 0010	0001 0000	0110 1100			
O	Time integral	5-0:0.8.5*255	Averaging duration for actual power value						
	–	h *or* min *or* sec		0000 cccc		0111 00nn			

This table consists of the cooling meter counts of combined heat/cooling meters (Medium = 0Dh). Refer to heat meter for heat meter counts.

	Heat	**6**	**04_h, $0C_h$, $0D_h$(heat)**	**(Heat only and combined heat/cooling)**				
M	Meter count	6-0:1.0.0*255	Energy (*A*), total, current value					
	–	kWh	10e-6 … 10e+1	0000 cccc	0000 0nnn			
	–	kWh	10e+2 … 10e+3	0000 cccc	1111 1011	0000 000n		
	–	kWh	10e+5 … 10e+6	0000 cccc	1111 1011	1000 000n	0111 1101	
	–	GJ	10e-9 … 10e-2	0000 cccc	0000 1nnn			
	–	GJ	10e-1 … 10e+0	0000 cccc	1111 1011	0000 100n		
	–	GJ	10e+2 … 10e+3	0000 cccc	1111 1011	1000 100n	0111 1101	
O	Meter count	6-0:1.2.0*255	Energy (*A*), total, set date value					
	–	kWh	10e-6 … 10e+1	0100 cccc	0000 0nnn			
	–	kWh	10e+2 … 10e+3	0100 cccc	1111 1011	0000 000n		
	–	kWh	10e+5 … 10e+6	0100 cccc	1111 1011	1000 000n	0111 1101	
	–	GJ	10e-9 … 10e-2	0100 cccc	0000 1nnn			
	–	GJ	10e-1 … 10e+0	0100 cccc	1111 1011	0000 100n		
	–	GJ	10e+2 … 10e+3	0100 cccc	1111 1011	1000 100n	0111 1101	
O	Power	6-0:8.0.0*255	Power (energy flow) (*P*), average, current value					
	–	W	10e-3 … 10e+4	0000 cccc	0010 1nnn			
	–	kJ/h	10e-3 … 10e+4	0000 cccc	0011 0nnn			
O	Flow rate	6-0:9.0.0*255	Flow rate, average (V_a/t), current value					
	–	m³/h	10e-6 … 10e+1	0000 cccc	0011 1nnn			
O	Time of count	6-0:0.9.1*255	Current time at time of transmission					
	–	Type F		0000 0100	0110 1101			
O	Date of count	6-0:0.9.2*255	Current date at time of transmission					
	–	Type G		0000 0010	0110 1100			
	–	Type F		0000 0100	0110 1101			
O	Date of count	6-0:0.1.10*255	Local date at set date					
	–	Type G		0100 0010	0110 1100			
O	Time integral	6-0:0.8.5*255	Averaging duration for actual power value					
	–	h *or* min *or* sec		0000 cccc	0111 00nn			

	Gas	**7**	**03_h**							
A1	Meter count	7-0:3.0.0*255	Volume (meter), measuring conditions (V_m), vorward, absolute, current value							
	–	m³	10e-6 … 10e+1	0000 cccc			1001 0nnn	0011 1010		
	–	m³	10e-3 … 10e+4	0000 cccc			1001 0nnn	1111 1101	0011 1010	
A1	Meter count	7-0:3.1.0*255	Volume (meter), temperature converted (V_{tc}), forward, absolute, current value							
	–	m³	10e-6 … 10e+1	0000 cccc			0001 0nnn			
	–	m³	10e-3 … 10e+4	0000 cccc			1001 0nnn	0111 1101		
A1	Meter count	7-0:3.2.0*255	Volume (meter), base conditions (V_b), forward, absolute, current value							
	–	m³	10e-6 … 10e+1	0000 cccc			1001 0nnn	0011 1110		
	–	m³	10e-3 … 10e+4	0000 cccc			1001 0nnn	1111 1101	0011 1110	
O	Meter count	7-0:3.0.0*VZ	Volume (meter), measuring conditions (V_m), forward, absolute, recent value							
	–	m³	10e-6 … 10e+1	1x00 cccc	1000 xxxx	0000 00xx	1001 0nnn	0011 1010		
	–	m³	10e-3 … 10e+4	1x00 cccc	1000 xxxx	0000 00xx	1001 0nnn	1111 1101	0011 1010	
O	Meter count	7-0:3.1.0*VZ	Volume (meter), temperature converted (V_{tc}), forward, absolute, recent value							
	–	m³	10e-6 … 10e+1	1x00 cccc	1000 xxxx	0000 00xx	0001 0nnn			
	–	m³	10e-3 … 10e+4	1x00 cccc	1000 xxxx	0000 00xx	1001 0nnn	0111 1101		
O	Meter count	7-0:3.2.0*VZ	Volume (meter), base conditions (V_b), forward, absolute, recent value							
	–	m³	10e-6 … 10e+1	1x00 cccc	1000 xxxx	0000 00xx	1001 0nnn	0011 1110		
	–	m³	10e-3 … 10e+4	1x00 cccc	1000 xxxx	0000 00xx	1001 0nnn	1111 1101	0011 1110	

O	Flow rate	7-0:43.15.0*255	Flow rate at measuring conditions, averaging period 1 (default period = 5 min), current interval (V_m/t_1)					
	–	m³/h	10e-6 … 10e+1	0000 cccc		1011 1nnn	0011 1010	
O	Flow rate	7-0:43.16.0*255	Flow rate, temperature converted, averaging period 1(default period = 5 min), current interval (V_{tc}/t_1)					
	–	m³/h	10e-6 … 10e+1	0000 cccc		0011 1nnn		
O	Flow rate	7-0:43.17.0*255	Flow rate at base conditions, averaging period 1 (default period = 5 min), current interval (V_b/t_1)					
	–	m³/h	10e-6 … 10e+1	0000 cccc		1011 1nnn	0011 1110	
O	Base temperature	7-0:41.2.0*255	defined Temperature, absolute, at base conditions (T_b) or for conversion (T_{tc})					
	–	°C	10e-3 … 10e+0	0000 cccc		1101 10nn	0011 1110	
O	Base pressure	7-0:42.2.0*255	defined Pressure, absolute, at base conditions (p_b)					
	–	bar	10e-3 … 10e+0	0000 cccc		1110 10nn	0011 1110	
	–	bar	10e-6 … 10e-3	0000 cccc		1110 10nn	1111 0011	0011 1110
O	Time of count	7-0:0.9.1*255	Current time at time of transmission					
	–	Type F		0000 0100		0110 1101		
O	Date of count	7-0:0.9.2*255	Current date at time of transmission					
	–	Type G		0000 0010		0110 1100		
	–	Type F		0000 0100		0110 1101		
O	Date of count	7-0:0.1.2*VZ	Local date at time of recent meter value, billing period 1 (default value = 1 day)					
	–	Type G		1x00 0010	1000 xxxx	0000 00xx	0110 1100	
	–	Type F		1x00 0100	1000 xxxx	0000 00xx	0110 1101	
O	Time integral	7-0:0.8.28*255	Averaging duration for actual flow rate value					
	–	h *or* min *or* sec		0000 cccc		0111 00nn		

	Cold Water	**8**	**07_h**				
M	Meter count	8-0:1.0.0*255	Volume (*V*), accumulated, total, current value				
	–	m³	10e-6 … 10e+1	0000 cccc	0001 0nnn		
	–	m³	10e-3 … 10e+4	0000 cccc	1001 0nnn	0111 1101	
O	Meter count	8-0:1.2.0*255	Volume (*V*), accumulated, total, set date value				
	–	m³	10e-6 … 10e+1	0100 cccc	0001 0nnn		
	–	m³	10e-3 … 10e+4	0100 cccc	1001 0nnn	0111 1101	
O	Flow rate	8-0:2.0.0*255	Flow rate, average (V_a/t), current value				
	–	m³/h	10e-6 … 10e+1	0000 cccc	0011 1nnn		
O	Time of count	8-0:0.9.1*255	Current time at time of transmission				
	–	Type F		0000 0100	0110 1101		
O	Date of count	8-0:0.9.2*255	Current date at time of transmission				
	–	Type G		0000 0010	0110 1100		
	–	Type F		0000 0100	0110 1101		
O	Date of count	8-0:0.1.10*255	Local date at set date				
	–	Type G		0100 0010	0110 1100		
O	Time integral	8-0:0.**8**.6*255	Averaging duration for actual flow rate value				
	–	h *or* min *or* sec		0000 cccc	0111 00nn		

	Hot Water	**9**	**06_h, 15_h**			
M	Meter count	9-0:1.0.0*255	Volume (V), accumulated, total, current value			
	–	m³	10e-6 … 10e+1	0000 cccc	0001 0nnn	
	–	m³	10e-3 … 10e+4	0000 cccc	1001 0nnn	0111 1101
O	Meter count	9-0:1.2.0*255	Volume (V), accumulated, total, set date value			
	–	m³	10e-6 … 10e+1	0100 cccc	0001 0nnn	
	–	m³	10e-3 … 10e+4	0100 cccc	1001 0nnn	0111 1101
O	Flow rate	9-0:2.0.0*255	Flow rate, average (V_a/t), current value			
	–	m³/h	10e-6 … 10e+1	0000 cccc	0011 1nnn	
O	Time of count	9-0:0.9.1*255	Current time at time of transmission			
	–	Type F		0000 0100	0110 1101	
O	Date of count	9-0:0.9.2*255	Current date at time of transmission			
	–	Type G		0000 0010	0110 1100	
	–	Type F		0000 0100	0110 1101	
O	Date of count	9-0:0.1.10*255	Local date at set date			
	–	Type G		0100 0010	0110 1100	
O	Time integral	9-0:0.**8**.6*255	Averaging duration for actual flow rate value			
	–	h *or* min *or* sec		0000 cccc	0111 00nn	

Annex B (Normative): OBIS-Declaration via the M-Bus

When a meter uses an M-Bus data point, which is not declared in Annex A and which is required for billing then it should assign the suggested OBIS-code for this data point as static data.

The OBIS-declaration uses the original DIF/VIF-combination of the declared M-Bus-data point added by the orthogonal VIFE “OBIS-declaration” (3Fh so far reserved). The value of this new data point consists of the assigned OBIS-code. The OBIS-code may be coded as BCD or binary value. It is declared in the low nibble of the original DIF (bold marked) which has to be replaced by length and coding of OBIS-code. (Use “binary” if recent value (OBIS-F)>99.)

Example1: Max. flow rate of a water meter

A water meter supports a maximum flow rate value e.g. 1.23 m3/h

The M-Bus data point for max. flow rate is coded as e.g.:

2**A**	DIF; maximum value; 4 digits BCD
33	VIF; Flow rate with unit 10-3 m3/h
23 01	Value 01.23

The relevant OBIS-Declaration will be transmitted as 12 digits BCD by

2**E**	DIF; maximum value; 12 digits BCD
B3	VIF; Flow rate with unit 10-3 m3/h; VIFE follows
3F	VIFE “OBIS-declaration”
AA 00 05 02 00 08	Value; OBIS-code 8-0:2.5.0*255

Note that the BCD Value “AA” in OBIS-field “F” signals an invalid value (refer to Annex A of [EN13757-3]). This corresponds to a recent value of 255.

Example 2: Special OBIS-code for status word of eHZ

The M-Bus data point for owner ship number is coded as e.g. 8 bit binary:

0**1**	DIF; 8 bit integer/binary
FD	VIFE code extension Table 11 in [EN13757-3]
17	Error flags (binary)
00	status value of 0000 0000b

The relevant OBIS-declaration will be transmitted e.g. as 48 bit binary by

0**6**	DIF; maximum value; 12 digits BCD
B3	VIF; flow rate with unit 10^{-3} m^3/h; VIFE follows
3F	VIFE “OBIS-declaration”
FF 05 05 60 00 01	Value; OBIS-code 1-0:96.5.5*255

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

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

- Support a minimum of 6 unit loads
  i.e. max operating current: 6*1.5mA+20mA (Space) = 29 mA
- Min. Mark voltage under mark/space current (max. 29mA): 23V
- Min. Space voltage under mark current (max.9mA): 12V
- Resulting max. idle power: 24V*9mA= 216 mW
- Baud rates: 300 and 2400 Baud
- Collision detect: For bus currents >30mA the bus voltage may drop below 23V. Bus currents >50mA shall be signaled 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 [EN13757-2]
- Symmetry as required in 4.3.3.10 of [EN13757-2]. DC symmetry requirements may be realized. This may be solved e.g. by a high resistance (2*1MOhm) voltage divider. AC-symmetry may be realized via a (parallel) capacitive divider of e.g.2*1nF.

Annex D (Informative): The Structure of the Application Header

The application header uses one of the following frame structures:

APL without Application 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

APL with Short Application Header

Full functionality; the meter application address is identical with the link address of the meter.

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

CI	ACC	STS	Sign.Word	AES-Check	Data

Applied from slave with 8Ah

CI	ACC	STS	Sign.Word

APL with Long Application Header

Full functionality; the meter application address differs from the link address of the meter (wM-Bus); the only application layer for M-Bus with support of mandatory secondary address.

- Applied from master with CI=5Bh; 60h; 65h; 6Ch, 6Dh, 80h
- Applied from slave with CI=72h; 7Ch; 7E; 8Bh

CI	Ident. no	Manuf.	Ver.	Med.	ACC	STS	Sign.Word	AES-Check	Data

Applied from master with 80h

Applied from slave with 8Bh

CI	Ident. no	Manuf.	Ver.	Med.	ACC	STS	Sign.Word

Explanation:

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 MUC access number; from slave initiated session uses meter access number)
STS	Status (from master to slave used for MUC-status (RSSI); from slave to master used for meter status)
Sign.Word	Signature word
AES-Check	2 Byte sequence 2Fh 2Fh for verification of successful encryption
Data	Application data; coding depends on used application protocol

Annex E (Normative): Application Error

Following additional error codes are defined as extension to standardised application errors in Table 14 of [EN13757-3] (2004):

Appl. error Code	***Meaning***	***Explanation***
16d	Access denied (Login, Password or Authorisation level is wrong)	Radio is an open unprotected medium. Therefore typically an authorisation with login and password is used. If a user applies wrong login or password or if the authorisation level of the user is too low for the requested command then this application error will be sent back.
17d	Application/Command unknown or not supported	occurs, when a user sends a command or a request to an application which is not implemented
18d	Parameter is missing or wrong	occurs, when a command is incomplete or has wrong parameter.
19d	Unknown Receiver address	A Bus device may retransmit/repeat data to the intended device. When this device is unknown it generates this error code.
20d	Decryption key fails	The decryption of the last command fails due to a wrong key. Slave returns this application error at the next request.
21d	Encryption method is not supported	The decryption of the last command fails. This Encryption method is not supported by the slave. Slave response this application error at the next request.
22d	Signature method is not supported	The authentication of the last command fails. This type of signature is not supported by the slave. Slave response this application error at the next request.
23d - 239d	Reserved	Reserved for future use
240d	Dynamic Application Error	The data point is coded as M-Bus-specific data point with a leading DIF/VIF. The declaration is vendor specific. The dynamic Appl. Error is limited to 7 bytes.
241d–255d	Manufacture specific Application error	The use of this Application error codes is vendor specific.

These application errors are currently defined in [EN13757-3] (2004) Table 14:

Application error Code	***Meaning***
0	Unspecified error: also if data field is missing
1	Unimplemented CI-Field
2	Buffer too long, truncated
3	Too many records
4	Premature end of record
5	More than 10 DIFE´s
6	More than 10 VIFE´s
7	Reserved
8	Application too busy for handling readout request
9	Too many readouts (for slaves with limited readouts per time)
10..255	Reserved

Annex F (Normative): Clock Synchronization

Two additional CI-fields (6Ch and 6Dh) shall be used to set a new date/time, or to do an incremental time correction independent of the application layer used otherwise. Since these are essentially SND_UD-type telegrams they shall be acknowledged by the meter by an ACK. They use the full 12 byte header that contains the application address of the slave (in addition to the MUC address in the link layer). The commands shall be encrypted using encryption mode 5 to prevent unauthorized date/time changes in the meter. This requires a block length of 16 bytes and decryption verification bytes. As usual the two leading 2Fh bytes shall be used for the decryption verification. The last four 2Fh filler bytes should be used for additional command verification. The date and time data formats I and J are defined in Annex A of [EN13757-3]. The TC-Field is used for control timing actions and is defined as:

Bit #	**Value**
0,1	00 (Bit1=0; Bit0=0) – set time 01 (Bit1=0; Bit0=1) – add time difference 10 (Bit1=1; Bit0=0) – subtract time difference 11 (Bit1=0; Bit0=0) – reserved
2..7	Reserved (0 by default)

1.) Set new date and time

CI=6Ch	Long APL-Header (12 byte)	AES-Check (2 byte= 2 * ”2Fh”)	TC-Field (1 byte) (set time)	Date/Time in Format I (6 byte, LSB first)	Reserved (3 bytes=0)	Command verification (4 byte = 4 * ”2Fh”)

Under metrological aspects this command is always considered as a clock reset by the slave.

2.) Add/Subtract Time Offset

Add/Subtract Time Offset to the current slave time to either correct a slave clock drift or to correct a possible slave time error due to a communication delay of a previous set date/time command.

CI=6Dh	Long APL-Header (12 byte)	AES-Check (2 byte= 2 * ”2Fh”)	TC-Field (1 byte) (add or subtract)	Time in Format J (3 byte, LSB first)	Reserved (6 bytes=0)	Command verification (4 byte = 4 * ”2Fh”)

If this command is received by the slave more than 60 sec after the last command or if the MUC access number is different from the last MUC-command, the add/subtract time command shall be executed, otherwise it is considered as a repetition of the last time correction command and shall be ignored.

The change of the meter clock should consider medium specific requirements as defined in dedicated standards and references. An example of clock synchronization telegram is listed in Annex M (SND-UD).

Annex G (Informative): Transmission of a Load Profile

When a meter generates a lot of periodical consumption values in one transmission it may be more efficient to transport a load profile instead of a list with pairs of consumption data and consumption value.

Example: Load profile of consumption values for a water meter

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

This load profile should be transmitted as follows:

Description	***DIF/DIFE (Hex)***	***VIF/VIFE (Hex)***	***Value (Hex) (Example)***
Count of transmitted Storage numbers (optional)	89 04	FD 22	05
Interval to the next storage number (here 1 month)	89 04	FD 28	01
Date of last storage number (#12)	82 06	6C	1F 15
Storage number #8	8C 04	13	65 00 00 00
Storage number #9	CC 04	13	09 02 00 00
Storage number #10	8C 05	13	23 04 00 00
Storage number #11	CC 05	13	55 07 00 00
Storage number #12	8C 06	13	13 10 00 00

The first transmitted data points are the profile parameter count, data and interval. Thereafter follows the cumulated consumption value per interval starting from the storage number #8. The lower storage numbers remains reserved for single values like the current consumption or the consumption at the due day etc.

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

Glossary

V_m	The volume at measurement conditions[5]
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) EN12405:2002 3.1.2
Base conditions	Fixed conditions used to express the volume of gas independently of the measurement conditions EN12405:2002 3.1.3
Converted volume	The converted volume from the quantity measured at metering conditions into a quantity at base conditions.

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}

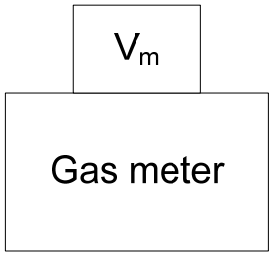
In general mentioned conversions can be done explicitly using devices measuring the specific condition or also implicitly by meters that measure independently from the specific condition.

To inform the billing center 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 VIF´s (e.g. “kWh”) together with the device type “gas” = 03h will provide such a clear indication which does not require further information.

[5] In German V_B is used instead of V_m, therefore care must be given to avoid confusion.

Volume at Measurement Conditions

All conversions are done solely at the billing center, 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.

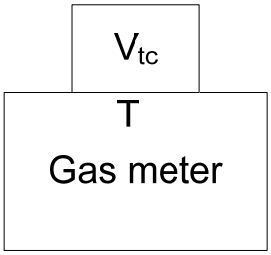
Suitable OBIS and M-Bus codes can be found in Annex A.

Temperature Converted Volume V_{tc}

An individual meter based volume conversion to V_{tc} (in contrast to the “global” billing center 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 center. Note that such a temperature conversion is based on a base temperature, which must be known to the billing center. 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 telegram.

Note that meter data can be converted by the billing center 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.

Temperature and Pressure Converted Volume

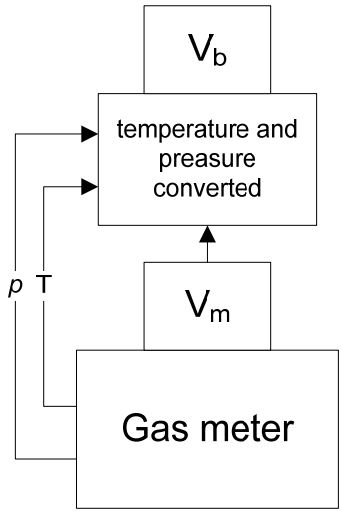
In addition to a volume conversion just regarding temperature an individual meter might convert its measured volume to base conditions regarding temperature and pressure. To comply with standard conditions, which are usually stated by national regulations and to allow the creation of gas bills that can 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 center. 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 telegram.

Note that meter data can be converted at the billing center 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.

OBIS / COSEM Application of Physical Units for Gas

(Extract from DLMS-UA Blue Book ed. 9)

Table 13 shows available physical units for the gas data objects given above.

By application of a scale factor (ref. table 4) the values can be scaled as required.

unit :: = enum	Unit	Quantity	Unit name	SI definition (comment)
(9)	°C	temperature (T)	Degree Celsius	K-273.15
(13)	m^3	volume (V) r_V , meter constant or pulse value (volume)	cubic metre	m^3
(14)	m^3	converted volume	cubic metre	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	

Table 13 – Enumerated values for physical units

Some examples are shown in Table 14 below.

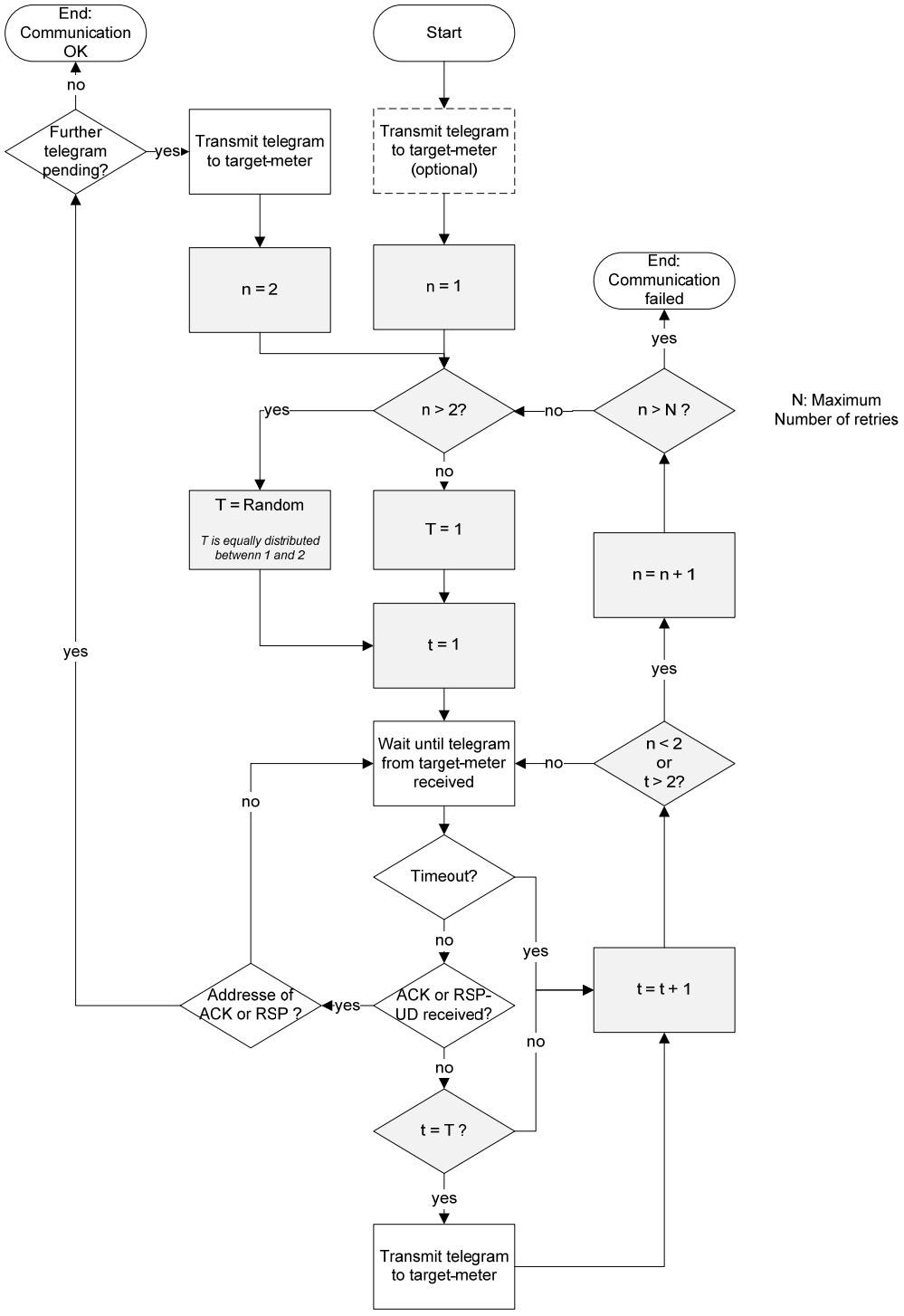
Value	Scaler	Unit	Data
263788	-3	m^3	263,788 m^3
593	3	Wh	593 kWh
3467	0	V	3467 V

Table 14 – Examples for scaler-unit

Annex I (Normative): Collision Avoiding Mechanism of the MUC

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 telegram types to prevent disturbing other conversations.

Flowchart



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 telegrams received during the actual try
- T Determines the telegram 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 telegram from the target meter to meet the following listen-after-talk window. The algorithm evaluates furthermore, if the telegram is related to an already ongoing conversation, which is the case if the telegram is an acknowledgment or a response. In this case, it is further evaluated if this telegram 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 telegram is neither part of another conversation nor the confirmation that a previous telegram was received, this would be an opportunity to send the telegram in case t equals T. Again, this latter additional condition resolves collision-scenarios with several devices transmitting simultaneously.

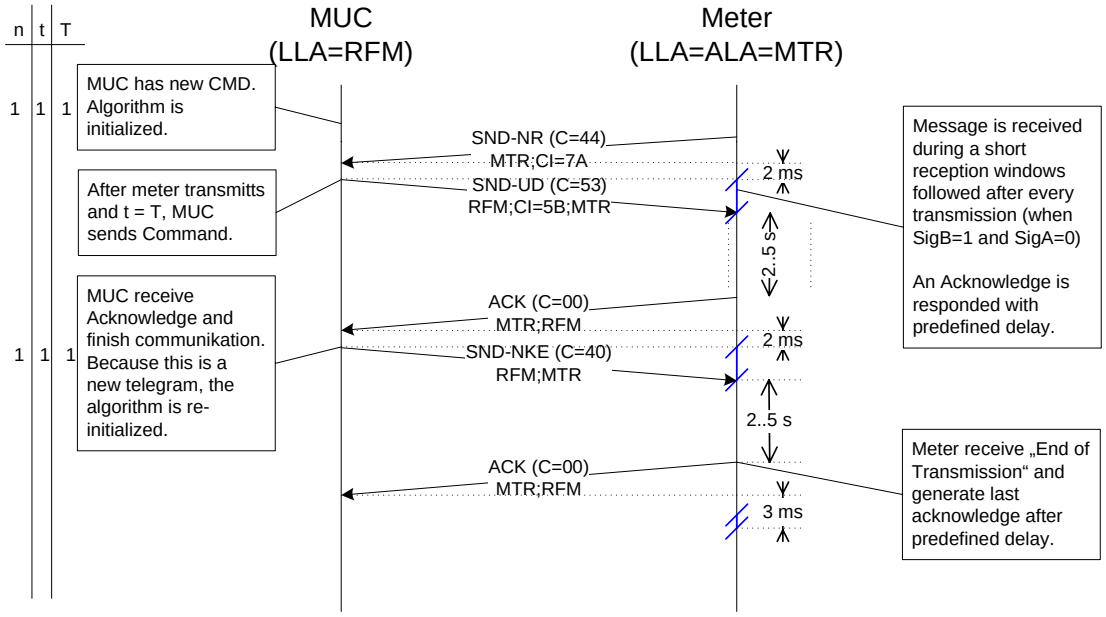
Example: Access of one MUC without Collision

Assume a scenario with only one MUC 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 telegram from the target meter is followed by the MUC's 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 telegram by the MUC. 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 behavior 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.

RF-Connection with Command (T-Mode)

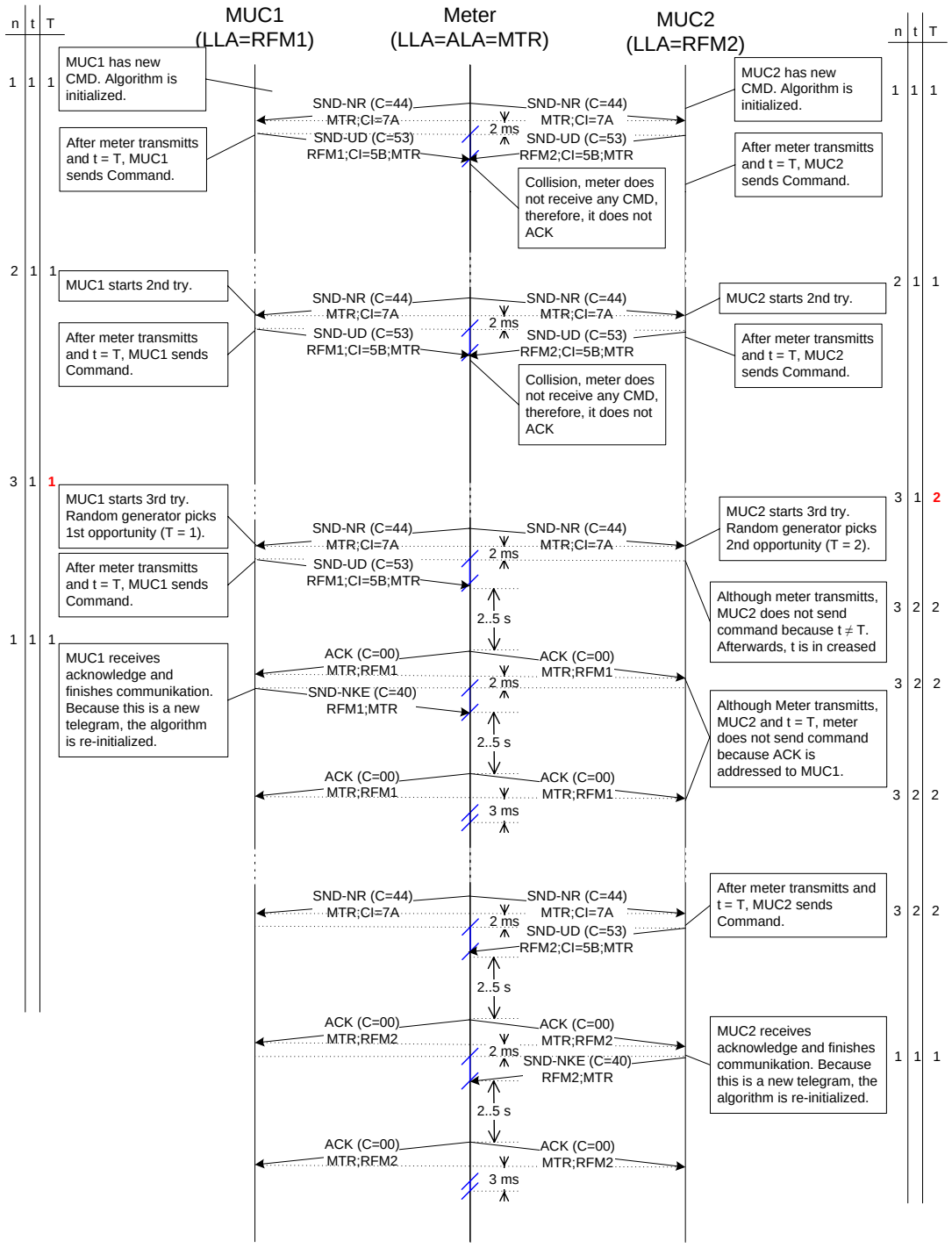


Example: Access of two MUCs with Collision

Assume a scenario with two MUCs and a meter, again with sufficient and equal radio propagation between the MUCs and the meter. Due to some reason, on both MUCs 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 MUCs initialize the algorithm in the same way. In our assumption the received field strength of both MUCs 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 telegrams 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 MUC determines T which now can be 1 or 2. Assuming a uniform distribution, there is a 50% probability that two MUCs choose different timeslots. This scenario is sketched in the following chart.

RF-Connection with Command (T-Mode)



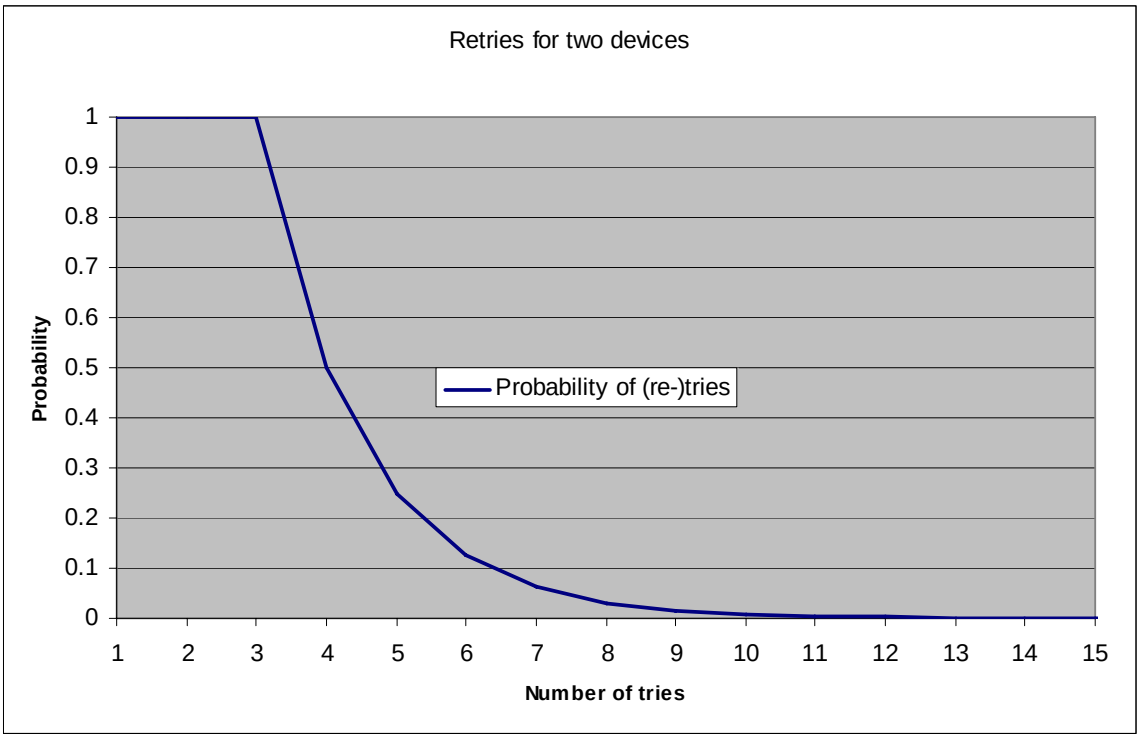
After the collision of the MUCs' first transmission, both start a 3rd try with MUC1 choosing the 1st and MUC2 the 2nd opportunity. As a result, MUC1 transmits the command after the next received telegram, whereas MUC2 waits for the next possibility. Because the following transmissions of the meter are dedicated to MUC1, MUC2 does not take these opportunities, although t is equivalent to T. Note that the received telegrams dedicated to another conversation do not result in incrementing t (see the flowchart of the algorithm). After this conversation with MUC1 is finished, MUC2 takes the next telegram originating from the meter to transmit its pending telegram.

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 $0.5^2 * 2 = 0.5$.

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 * 1 * 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 $1 * 0.5^{n-2}$ (for n > 2)



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 * 2 = 20.

Annex K (Informative): Example of Message Types

	First block								Second block and…						
	L	**C**	Manuf	Ident number	Ver	Med	CRC	**CI**	Ident number	Manuf	Ver	Med	Access	Status	Signatur	
				Meter Link-Addr.					*Meter Appl.-Addr.*				*MTR-ACC*	*MTR-ST*	*Sign.word*	*Data*
SND_NR	xx	44	B3 3D	44 33 22 11	55	0F	CRC	72	55 66 77 88	B3 3D	44	07	B1	00	20 85	{2F 2F DIF} CRC {VIF …}CRC

				MUC-Addr.					*Meter Appl.-Addr.*				*MUC-ACC*	*MUC-ST*	*Sign.word*	*Data*
REQ_UD2	16	5B	A3 36	78 56 34 12	9A	31	CRC	80	55 66 77 88	B3 3D	44	07	A0	00	00 C0	CRC
				Meter Link-Addr.					*Meter APL-Addr.*				*MUC-ACC*	*MTR-ST*	*Sign.word*	*Data*
RSP_UD	xx	08	B3 3D	44 33 22 11	55	0F	CRC	72	55 66 77 88	B3 3D	44	07	A0	00	30 85	{2F 2F DIF} CRC {VIF …}CRC

				MUC-Addr.					*Meter Appl.-Addr.*				*MUC-ACC*	*MUC-ST*	*Sign.word*	*Data*
SND_UD	xx	73	A3 36	78 56 34 12	9A	31	CRC	5B	55 66 77 88	B3 3D	44	07	A1	00	10 C5	{2F 2F DIF} CRC {VIF …}CRC
				Meter Link-Addr.					*Meter Appl.-Addr.*				*MUC-ACC*	*MTR-ST*	*Sign.word*	*no data*
ACK	16	00	B3 3D	44 33 22 11	55	0F	CRC	8B	55 66 77 88	B3 3D	44	07	A1	00	00 80	CRC

				MUC-Addr.					*Meter Appl.-Addr.*				*MUC-ACC*	*MUC-ST*	*Sign.word*	*No data*
SND_NKE	16	40	A3 36	78 56 34 12	9A	31	CRC	80	55 66 77 88	B3 3D	44	07	A2	00	00 C0	CRC
				Meter Link-Addr.					*Meter Appl.-Addr.*				*MUC-ACC*	*MTR-ST*	*Sign.word*	*No data*
ACK	16	00	B3 3D	44 33 22 11	55	0F	CRC	8B	55 66 77 88	B3 3D	44	07	A2	00	00 80	CRC

				Meter Link-Addr.					*Meter APL-Addr.*				*MTR-ACC*	*MTR-ST*	*Sign.word*	*Data*
SND_IR	xx	46	B3 3D	66 55 44 33	77	03	CRC	7A					C2	00	20 85	{2F 2F DIF} CRC {VIF …}CRC
				MUC-Addr.					*Meter Appl.-Addr.*				*MTR-ACC*	*MUC-ST*	*Sign.word*	*No data*
SND-IC	16	06	A3 36	78 56 34 12	9A	31	CRC	80	66 55 44 33	B3 3D	77	03	C2	00	00 C0	CRC

				Meter Link-Addr.					*Meter APL-Addr.*				*MTR-ACC*	*MTR-ST*	*Sign.word*	*No data*
ACC-DMD	0E	40	B3 3D	66 55 44 33	77	03	CRC	8A					C3	00	00 80	CRC
				MUC-Addr.					*Meter Appl.-Addr.*				*MTR-ACC*	*MUC-ST*	*Sign.word*	*No data*
ACK	16	06	A3 36	78 56 34 12	9A	31	CRC	80	66 55 44 33	B3 3D	77	03	C3	00	00 C0	CRC

5

Address of example devices:

MUC

Manuf	13987d	36A3h	"MUC"
Ident	12345678d	12 34 56 78h	BCD-Coding!
Version	154d	9Ah	Binäry
Medium	49d	31h	"System"

Gas-Meter with integrated RF-Modul (M-Bus)

Manuf	15795d	3DB3h	"OMS"
Ident	33445566d	33 44 55 66h	BCD-Coding!
Version	119d	77h	Binäry
Medium	03d	03h	"Gas"

Meter w/o RF (M-Bus)

Manuf	15795d	3DB3h	"OMS"
Ident	88776655d	88 77 66 55h	BCD-Coding!
Version	68d	44h	Binäry
Medium	07d	07h	"Water"

together with

ext. RF-Adapter for Water

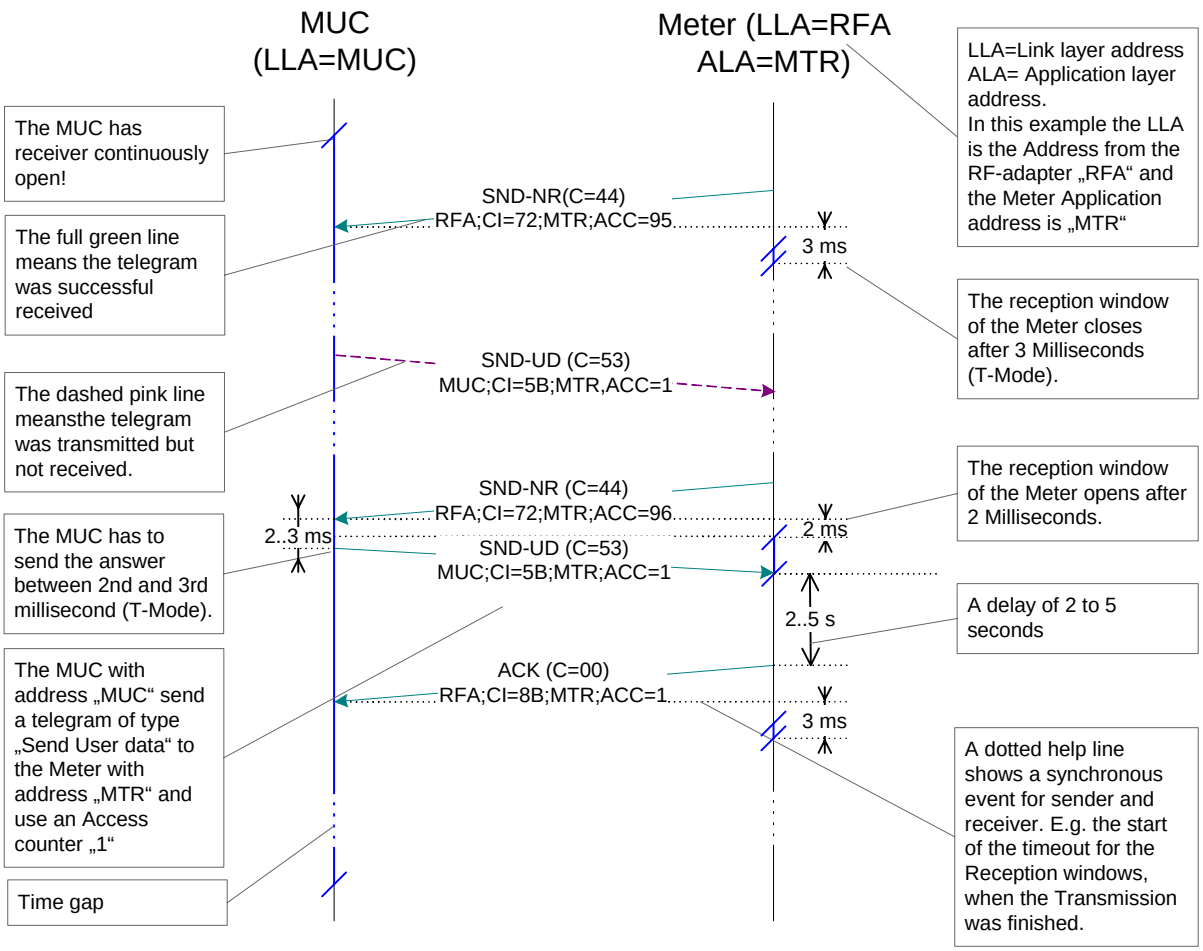
Manuf	15795d	3DB3h	"OMS"
Ident	11223344d	11 22 33 44h	BCD-Coding!
Version	85d	55h	Binäry
Medium	15d	0Fh	"unknown"

Annex L (Normative): Timing Diagram

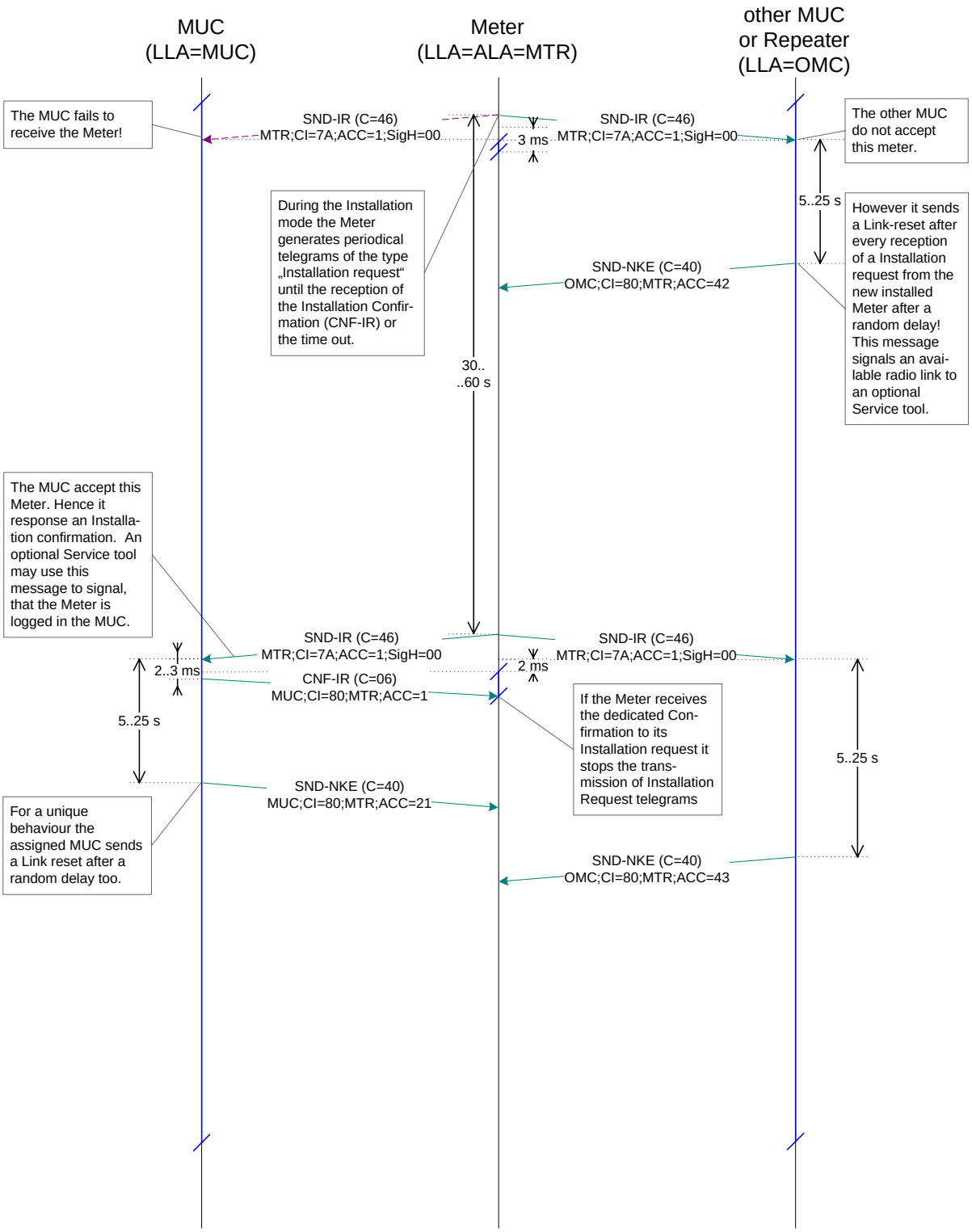
The next pages show examples of Timing diagrams. Some of the examples are made for S-mode and others for T-mode. However the examples may apply even for the alternative mode. The different access timing of alternative reception windows has to be considered.

5

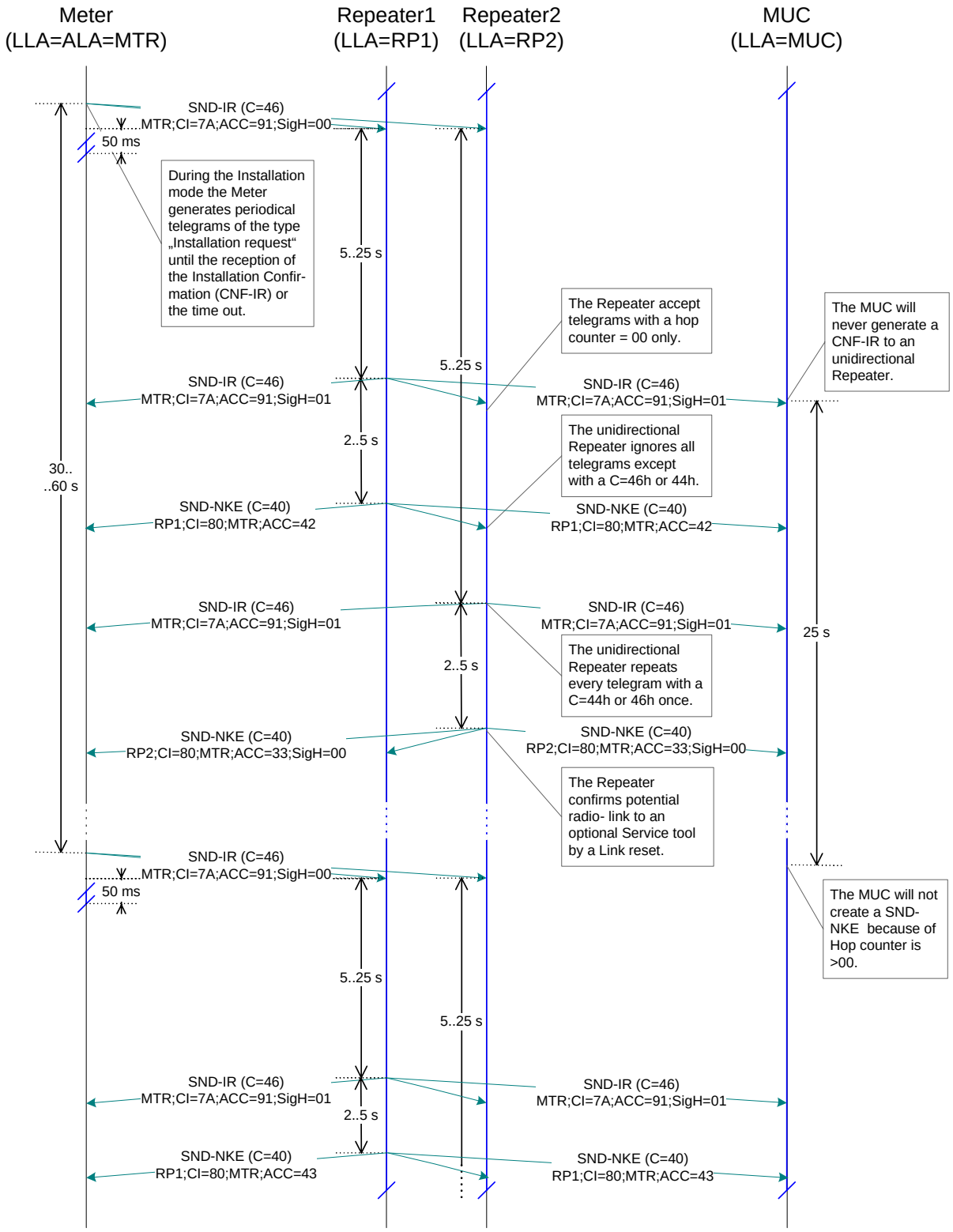
Legend



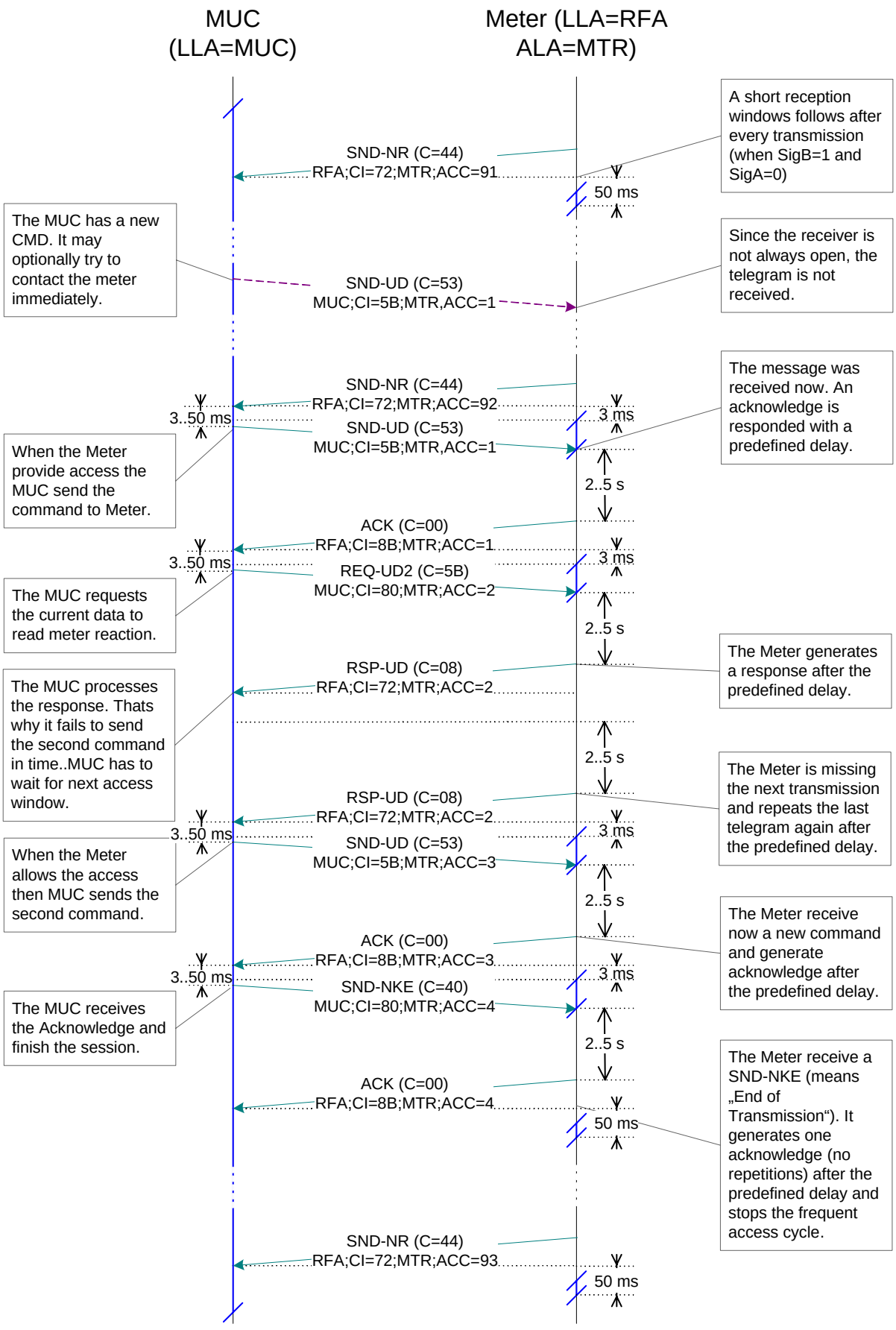
Installation Procedure (T-Mode)



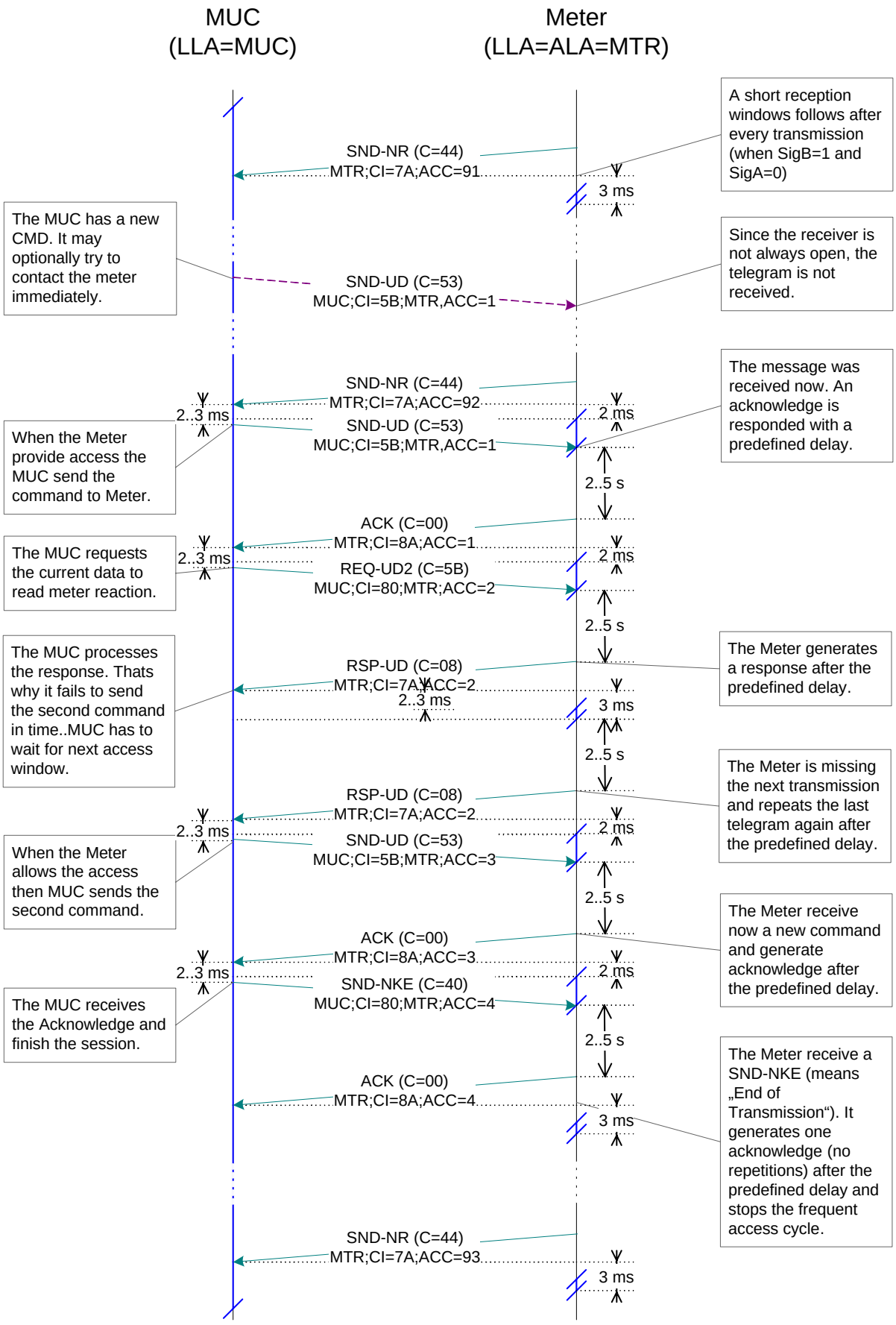
Installation Procedure with Unidirectional Repeaters (S-Mode)



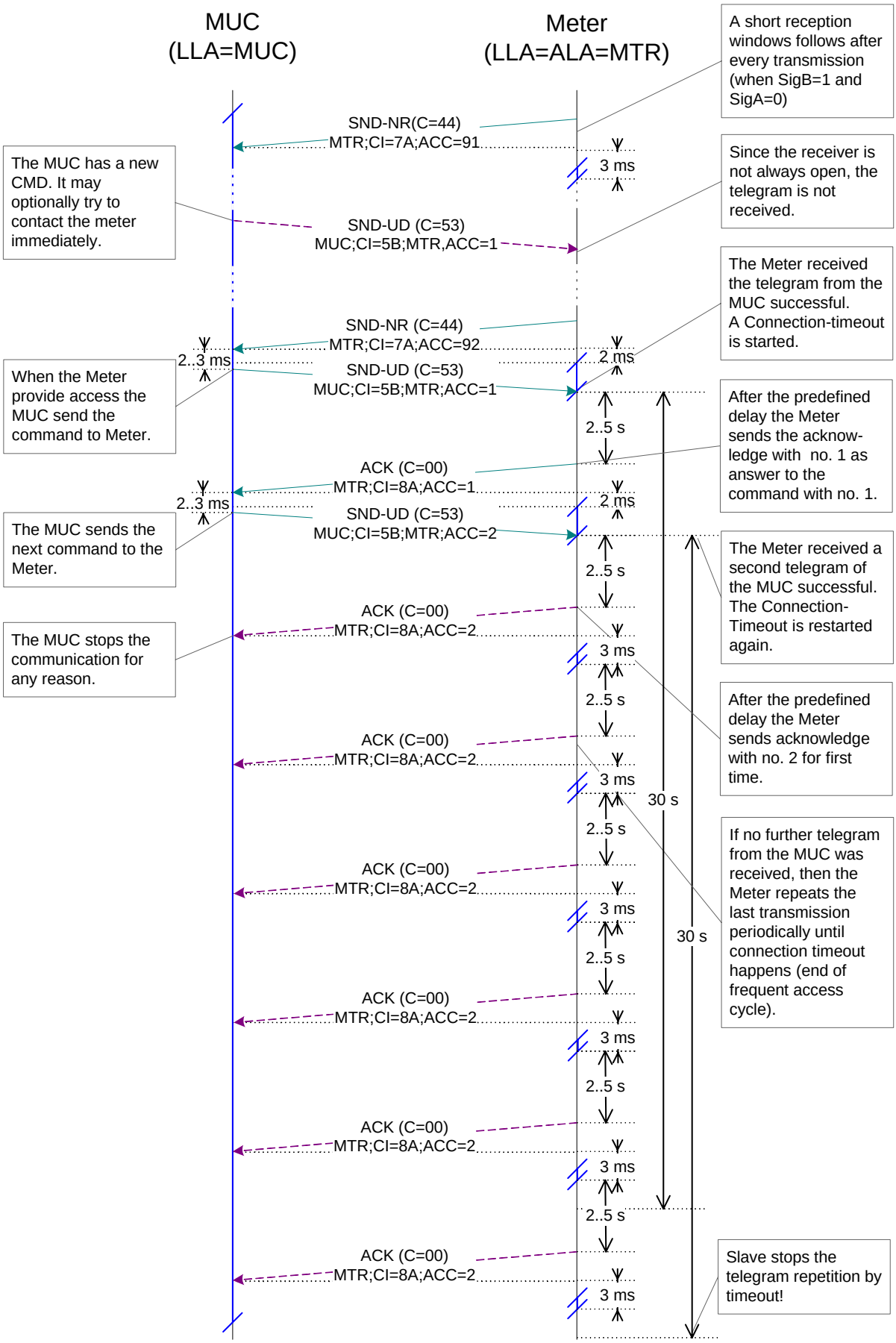
RF-Connection with Long Address (S-Mode)



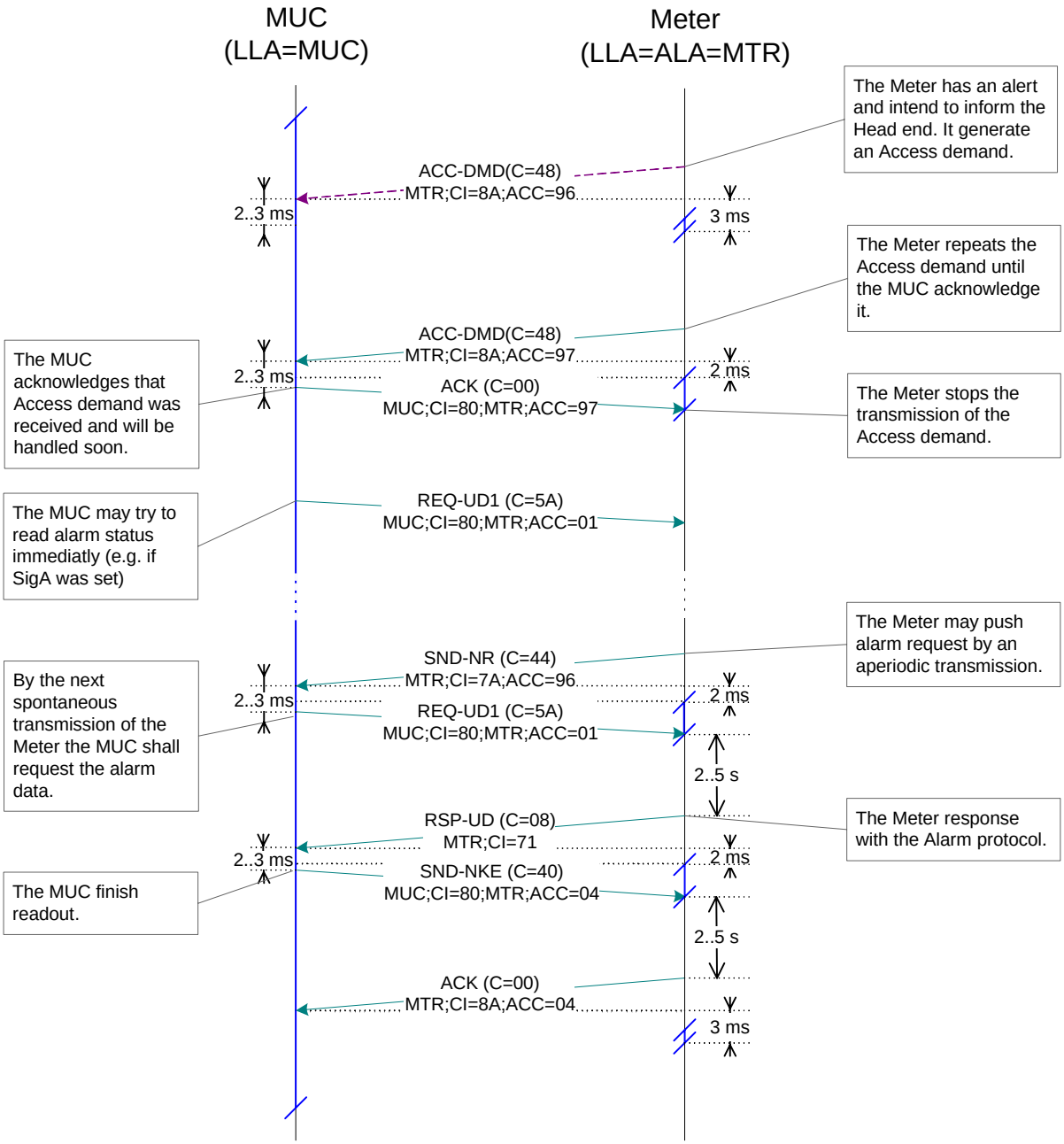
RF-Connection with Short Address (T-Mode)



Connection Timeout after Command (T-Mode)



Access Demand from Meter (T-Mode)



Annex M (Informative):
Telegram Examples for the M-Bus and the wM-Bus

Gas Meter

Gas meter example	
Medium	Gas
Manufacturer	ELS
Serial number	12345678
Version	51
Forward absolute meter volume	28504,27 m²
date and time of read out	31.05.2008 23:50
Error code binary	0

AES Key according to FIPS 197 (LSB first):
= manu. spec. at least 8 bytes unique for each meter
= 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 11

AES CBC Initial Vector according to FIPS 197 (LSB first):
= M Field + A Field + 8 bytes Acces No
= 93 15 78 56 34 12 33 03 2A 2A 2A 2A 2A 2A 2A 2A

SND_NR (wM-Bus)

		OMS wM-Bus frame	Gas meter example		
Byte No	Field Name	Content	Bytes [hex]	Bytes [hex]	
			plain	AES coded	
1	L Field	Length of data (46 bytes)	2Eh	2Eh	Linklayer (DLL)
2	C Field	44h in Normal mode	44h	44h	
3	M Field	Manufacturer code	93h	93h	
4	M Field	Manufacturer code	15h	15h	
5	A Field	Serial No LSB (BCD)	78h	78h	
6	A Field	Serial No (BCD)	56h	56h	
7	A Field	Serial No (BCD) (= 12345678)	34h	34h	
8	A Field	Serial No MSB (BCD)	12h	12h	
9	A Field	Version (or Generation number)	33h	33h	
10	A Field	Device type (Medium=Gas)	03h	03h	
11	CRC 1		33h	33h	
12	CRC 1		63h	63h	

13	CI Field	7Ah means 4 bytes header	7Ah	7Ah	Application layer (APL)
14	Access No.	Transmission counter	2Ah	2Ah	
15	Status	M-Bus state contents errors and alerts	00h	00h	
16	Signature	NNNNCCHHb (2 encr. blocks)	00h	20h	
17	Signature	BA00MMMMb (unidir., AES)	00h	05h	
18	AES-Verify	Encryption verification	2Fh	59h	AES-Encrypted Block 1
19	AES-Verify	Encryption verification	2Fh	23h	
20	DR1	DIF (8 digit BCD)	0Ch	C9h	
21	DR1	VIF (Volume 0,01 m³)	14h	5Ah	
22	DR1	Value LSB	27h	AAh	
23	DR1	Value	04h	26h	
24	DR1	Value (= 28504,27 m³)	85h	D1h	
25	DR1	Value MSB	02h	B2h	
26	DR2	DIF (Time at readout; Type F)	04h	E7h	
27	DR2	VIF (Date, Time)	6Dh	49h	
28	DR2	Value LSB	32h	3Bh	
29	CRC 2		16h	2Ah	DLL
30	CRC 2		7Fh	8Bh	
31	DR2	Value	37h	01h	Application layer (APL)
32	DR2	Value (31.05.2008 23:50)	1Fh	3Eh	
33	DR2	Value MSB	15h	C4h	
34	DR3	DIF (2 byte integer)	02h	A6h	
35	DR3	VIF (VIF-Extension Table FD)	FDh	F6h	
36	DR3	VIFE (error flag)	17h	D3h	AES-Encrypted Block 2
37	DR3	Value LSB	00h	52h	
38	DR3	Value MSB (= 0)	00h	9Bh	
39	Dummy	Fill Byte due to AES	2Fh	52h	
40	Dummy	Fill Byte due to AES	2Fh	0Eh	
41	Dummy	Fill Byte due to AES	2Fh	DFh	
42	Dummy	Fill Byte due to AES	2Fh	F0h	
43	Dummy	Fill Byte due to AES	2Fh	EAh	
44	Dummy	Fill Byte due to AES	2Fh	6Dh	
45	Dummy	Fill Byte due to AES	2Fh	EFh	
46	Dummy	Fill Byte due to AES	2Fh	C9h	
47	CRC 3		E1h	55h	DLL
48	CRC 3		B3h	B2h	
49	Dummy	Fill Byte due to AES	2Fh	9Dh	Application layer (APL)
50	Dummy	Fill Byte due to AES	2Fh	6Dh	
51	Dummy	Fill Byte due to AES	2Fh	69h	
52	Dummy	Fill Byte due to AES	2Fh	EBh	
53	Dummy	Fill Byte due to AES	2Fh	F3h	
54	CRC 4		25h	ECh	DLL
55	CRC 4		EEh	8Ah	

RSP_UD (M-Bus)

Byte No		OMS M-Bus frame	Gas meter example	
	Field Name	Content	Bytes [hex]	
			plain	
1	Start	Start byte	68h	Linklayer (DLL)
2	L Field	Length of data (32 bytes)	20h	
3	L Field	Length of data (32 bytes)	20h	
4	Start	Start byte	68h	
5	C Field	Respond user data	08h	
6	A-Field	Secondary addressing mode	FDh	
7	CI Field	72h means 12 bytes header	72h	Application layer (APL)
8	Ident.Nr.	Serial No LSB (BCD)	78h	
9	Ident.Nr.	Serial No (BCD)	56h	
10	Ident.Nr.	Serial No (BCD) (=12345678)	34h	
11	Ident.Nr.	Serial No MSB (BCD)	12h	
12	Manufr	Manufacturer code	93h	
13	Manufr	Manufacturer code	15h	
14	Version	Version (or Generation number)	33h	
15	Device type	Device type (Medium=Gas)	03h	
16	Access No.	Transmission counter	2Ah	
17	Status	M-Bus state contents errors and alerts	00h	
18	Signature	no Encryption	00h	
19	Signature	no Encryption	00h	
20	DR1	DIF (8 digit BCD)	0Ch	
21	DR1	VIF (Volume 0,01 m²)	14h	
22	DR1	Value LSB	27h	
23	DR1	Value	04h	
24	DR1	Value (= 28504,27 m²)	85h	
25	DR1	Value MSB	02h	
26	DR2	DIF (Time at readout; Type F)	04h	
27	DR2	VIF (Date, Time)	6Dh	
28	DR2	Value LSB	32h	
29	DR2	Value	37h	
30	DR2	Value (31.05.2008 23:50)	1Fh	
31	DR2	Value MSB	15h	
32	DR3	DIF (2 byte integer)	02h	
33	DR3	VIF (FD-Table)	FDh	
34	DR3	VIFE (error flag)	17h	
35	DR3	Value LSB	00h	
36	DR3	Value MSB (= 0)	00h	
37	Checksum		89h	DLL
38	Stop	Stop byte	16h	

Water Meter

Water meter example	
Medium	Water
Manufacturer	HYD
Serial number	92752244
Version	41
Main volume counter	2850427 l
Volume flow	127 l/h
Volume counter at set date	1445419 l
set date	31.04.2007
Error code binary	0

AES Key According to FIPS 197 (LSB first):
= manu. spec. at least 8 bytes unique for each meter = 82 B0 55 11 91 F5 1D 66 EF CD AB 89 67 45 23 01

AES CBC Initial Vector according to FIPS 197 (LSB first):
= M Field + A Field + 8 bytes Acces No = 24 23 44 22 75 92 29 07 1F 1F 1F 1F 1F 1F 1F 1F

5

SND_NR (wM-Bus)

		OMS wM-Bus frame	Water meter example		
Byte No	Field Name	Content	Bytes [hex]	Bytes [hex]	
			plain	AES coded	
1	L Field	Length of data (46 bytes)	2Eh	2Eh	Linklayer (DLL)
2	C Field	44h in Normal mode	44h	44h	
3	M Field	Manufacturer code	24h	24h	
4	M Field	Manufacturer code	23h	23h	
5	A Field	Serial No LSB (BCD)	44h	44h	
6	A Field	Serial No (BCD)	22h	22h	
7	A Field	Serial No (BCD) (= 92752244)	75h	75h	
8	A Field	Serial No MSB (BCD)	92h	92h	
9	A Field	Version (or Generation number)	29h	29h	
10	A Field	Device type (Medium=Water)	07h	07h	
11	CRC 1		38h	38h	
12	CRC 1		D1h	D1h	

13	CI Field	7Ah means 4 bytes header	7Ah	7Ah	Application layer (APL)
14	Access No.	Transmission counter	1Fh	1Fh	
15	Status	M-Bus state contents errors and alerts	00h	00h	
16	Signature	NNNNCCHHb (2 encr. blocks)	00h	20h	
17	Signature	BA00MMMMb (unidir., AES)	00h	05h	
18	AES-Verify	Encryption verification	2Fh	05h	AES-Encrypted Block 1
19	AES-Verify	Encryption verification	2Fh	9Bh	
20	DR1	DIF (8 digit BCD)	0Ch	4Dh	
21	DR1	VIF (Volume liter)	13h	12h	
22	DR1	Value LSB	27h	F7h	
23	DR1	Value (= 2850427)	04h	35h	
24	DR1	Value	85h	5Eh	
25	DR1	Value MSB	02h	4Dh	
26	DR2	DIF (6 digit BCD)	0Bh	F6h	
27	DR2	VIF (Volume flow l/h)	3Bh	DFh	
28	DR2	Value LSB	27h	4Ch	
29	CRC 2		15h	FFh	DLL
30	CRC 2		83h	36h	
31	DR2	Value (= 127)	01h	67h	Application layer (APL)
32	DR2	Value MSB	00h	BEh	
33	DR3	DIF (8 digit BCD, StorageNo 1)	4Ch	FBh	
34	DR3	VIF (Volume liter)	13h	7Ah	
35	DR3	Value LSB	19h	54h	
36	DR3	Value (= 1445419)	54h	76h	AES-Encrypted Block 2
37	DR3	Value	44h	11h	
38	DR3	Value MSB	01h	2Fh	
39	DR4	DIF (Data type G, StorageNo 1)	42h	F4h	
40	DR4	VIF (Date)	6Ch	48h	
41	DR4	Value LSB	FFh	BFh	
42	DR4	Value MSB (= 31.12.2007)	0Ch	98h	
43	DR5	DIF (2 byte integer)	02h	1Ah	
44	DR5	VIF (FD-Table)	FDh	F9h	
45	DR5	VIFE (error flag)	17h	06h	
46	DR5	Value LSB	00h	4Ch	
47	CRC 3		DAh	B7h	DLL
48	CRC 3		B5h	43h	
49	DR5	Value MSB (= 0)	00h	0Ah	Application layer (APL)
50	Dummy	Fill Byte due to AES	2Fh	CDh	
51	Dummy	Fill Byte due to AES	2Fh	43h	
52	Dummy	Fill Byte due to AES	2Fh	A1h	
53	Dummy	Fill Byte due to AES	2Fh	97h	
54	CRC 4		BDh	CBh	DLL
55	CRC 4		18h	FDh	

RSP_UD (M-Bus)

Byte No		OMS M-Bus frame	Water meter example	
	Field Name	Content	Bytes [hex]	
			plain	
1	Start	Start byte	68h	Linklayer (DLL)
2	L Field	Length of data (41 bytes)	29h	
3	L Field	Length of data (41 bytes)	29h	
4	Start	Start byte	68h	
5	C Field	Respond user data	08h	
6	A-Field	Secondary addressing mode	FDh	
7	CI Field	72h means 12 bytes header	72h	Application layer (APL)
8	Ident.Nr.	Serial No LSB (BCD)	44h	
9	Ident.Nr.	Serial No (BCD)	22h	
10	Ident.Nr.	Serial No (BCD) (=12345678)	75h	
11	Ident.Nr.	Serial No MSB (BCD)	92h	
12	Manufr	Manufacturer code	24h	
13	Manufr	Manufacturer code	23h	
14	Version	Version (or Generation number)	29h	
15	Device type	Device type (Medium=Water)	07h	
16	Access No.	Transmission counter	1Fh	
17	Status	M-Bus state contents errors and alerts	00h	
18	Signature	no Encryption	00h	
19	Signature	no Encryption	00h	
20	DR1	DIF (8 digit BCD)	0Ch	
21	DR1	VIF (Volume liter)	13h	
22	DR1	Value LSB	27h	
23	DR1	Value (= 2850427)	04h	
24	DR1	Value	85h	
25	DR1	Value MSB	02h	
26	DR2	DIF (6 digit BCD)	0Bh	
27	DR2	VIF (Volume flow l/h)	3Bh	
28	DR2	Value LSB	27h	
29	DR2	Value (= 127)	01h	
30	DR2	Value MSB	00h	
31	DR3	DIF (8 digit BCD, StorageNo 1)	4Ch	
32	DR3	VIF (Volume liter)	13h	
33	DR3	Value LSB	19h	
34	DR3	Value (= 1445419)	54h	
35	DR3	Value	44h	
36	DR3	Value MSB	01h	
37	DR4	DIF (Data type G, StorageNo 1)	42h	
38	DR4	VIF (Date)	6Ch	
39	DR4	Value LSB	FFh	
40	DR4	Value MSB (= 31.12.2007)	0Ch	
41	DR5	DIF (2 byte integer)	02h	
42	DR5	VIF (FD-Table)	FDh	
43	DR5	VIFE (error flag)	17h	
44	DR5	Value LSB	00h	
45	DR5	Value MSB (= 0)	00h	
46	Checksum		99h	DLL
47	Stop	Stop byte	16h	

Heat Meter

Heat meter example	
Medium	Heat (outlet)
Manufacturer	HYD
Serial number	12345678
Version	42
Main energy counter	2850427 kWh
Main volume counter	703476 l
Energy counter at set date	1445419 kWh
set date	31.12.2007
Volume flow	127 l/h
Power	329,7 W
Flow temperature	44,3 °C
Return temperature	25,1 °C
Error code binary	0

AES Key According to FIPS 197 (LSB first):
= manu. spec. at least 8 bytes unique for each meter
= D3 51 D9 0E 58 C8 E8 C8 EF CD AB 89 67 45 23 01

AES CBC Initial Vector according to FIPS 197 (LSB first):
= M Field + A Field + 8 bytes Acces No
= 24 23 78 56 34 12 2A 04 26 26 26 26 26 26 26 26

5

SND_NR (wM-Bus)

		OMS wM-Bus frame	Heat meter example		
Byte No	Field Name	Content	Bytes [hex]	Bytes [hex]	
			plain	AES coded	
1	L Field	Length of data (62 bytes)	3Eh	3Eh	Linklayer (DLL)
2	C Field	44h in Normal mode	44h	44h	
3	M Field	Manufacturer code	24h	24h	
4	M Field	Manufacturer code	23h	23h	
5	A Field	Serial No LSB (BCD)	78h	78h	
6	A Field	Serial No (BCD)	56h	56h	
7	A Field	Serial No (BCD) (=12345678)	34h	34h	
8	A Field	Serial No MSB (BCD)	12h	12h	
9	A Field	Version (or Generation number)	2Ah	2Ah	
10	A Field	Device type (Medium=Heat_outlet)	04h	04h	
11	CRC 1		9Dh	9Dh	
12	CRC 1		CCh	CCh	
13	CI Field	7Ah means 4 bytes header	7Ah	7Ah	
14	Access No.	Transmission counter	26h	26h	
15	Status	M-Bus state contents errors and alerts	00h	00h	
16	Signature	NNNNCCHHb (3 encr. blocks)	00h	30h	
17	Signature	BA00MMMMb (unidir., AES)	00h	05h	

18	AES-Verify	Encryption verification	2Fh	92h	AES-Encrypted Block 1	
19	AES-Verify	Encryption verification	2Fh	A9h		
20	DR1	DIF (8 digit BCD)	0Ch	7Fh		
21	DR1	VIF (Energy kWh)	06h	11h		
22	DR1	Value LSB	27h	B4h		
23	DR1	Value (= 2850427)	04h	7Ah		
24	DR1	Value	85h	E8h		
25	DR1	Value MSB	02h	5Eh		
26	DR2	DIF (8 digit BCD)	0Ch	72h		
27	DR2	VIF (Volume liter)	13h	B2h		
28	DR2	Value LSB	76h	01h		
29	CRC 2		6Bh	FAh	DLL	
30	CRC 2		35h	91h		
31	DR2	Value (= 703476)	34h	C6h		Application layer (APL)
32	DR2	Value	70h	AAh		
33	DR2	Value MSB	00h	64h		
34	DR3	DIF (8 digit BCD, StorageNo 1)	4Ch	43h		
35	DR3	VIF (Energy kWh)	06h	82h		
36	DR3	Value LSB	19h	8Bh	AES-Encrypted Block 2	
37	DR3	Value (= 1445419)	54h	E7h		
38	DR3	Value	44h	1Bh		
39	DR3	Value MSB	01h	B9h		
40	DR4	DIF (Data type G, StorageNo 1)	42h	ECh		
41	DR4	VIF (Date)	6Ch	F1h		
42	DR4	Value LSB	FFh	BAh		
43	DR4	Value MSB (= 31.12.2007)	0Ch	E8h		
44	DR5	DIF (6 digit BCD)	0Bh	A0h		
45	DR5	VIF (Volume flow l/h)	3Bh	74h		
46	DR5	Value LSB	27h	E9h		
47	CRC 3		19h	E1h	DLL	
48	CRC 3		04h	29h		
49	DR5	Value (= 127)	01h	86h		
50	DR5	Value MSB	00h	Abh		
51	DR6	DIF (6 digit BCD)	0Bh	FAh		
52	DR6	VIF (Power 100 mW)	2Ah	44h		
53	DR6	Value LSB	97h	8Dh		
54	DR6	Value (= 3297)	32h	DAh	AES-Encrypted Block 3	
55	DR6	Value MSB	00h	BCh		
56	DR7	DIF (4 digit BCD)	0Ah	ECh		
57	DR7	VIF (Flow Temp. 100 m°C)	5Ah	F6h		
58	DR7	Value LSB	43h	17h		
59	DR7	Value MSB (= 443)	04h	50h		
60	DR8	DIF (4 digit BCD)	0Ah	05h		
61	DR8	VIF (Return Temp. 100 m°C)	5Eh	59h		
62	DR8	Value LSB	51h	22h		
63	DR8	Value MSB (= 251)	02h	85h		
64	DR9	DIF (2 byte integer)	02h	2Eh		
65	CRC 4		7Dh	0Eh	DLL	
66	CRC 4		68h	CDh		
67	DR9	VIF (FD-Table)	FDh	93h		
68	DR9	VIFE (error flag)	17h	B9h		
69	DR9	Value LSB	00h	B2h		
70	DR9	Value MSB (= 0)	00h	ABh		
71	Dummy	Fill Byte due to AES	2Fh	76h		
72	CRC 5		D7h	51h	DLL	
73	CRC 5		DBh	A6h		

RSP_UD (M-Bus)

Byte No		OMS M-Bus frame	Heat meter example	
	Field Name	Content	Bytes [hex]	
			plain	
1	Start	Start byte	68h	Linklayer (DLL)
2	L Field	Length of data (60 bytes)	3Ch	
3	L Field	Length of data (60 bytes)	3Ch	
4	Start	Start byte	68h	
5	C Field	Respond user data	08h	
6	A-Field	Secondary addressing mode	FDh	
7	CI Field	72h means 12 bytes header	72h	Application layer (APL)
8	Ident.Nr.	Serial No LSB (BCD)	78h	
9	Ident.Nr.	Serial No (BCD)	56h	
10	Ident.Nr.	Serial No (BCD) (=12345678)	34h	
11	Ident.Nr.	Serial No MSB (BCD)	12h	
12	Manufr	Manufacturer code	24h	
13	Manufr	Manufacturer code	23h	
14	Version	Version (or Generation number)	2Ah	
15	Device type	Device type (Medium=Heat_outlet)	04h	
16	Access No.	Transmission counter	26h	
17	Status	M-Bus state contents errors and alerts	00h	
18	Signature	no Encryption	00h	
19	Signature	no Encryption	00h	
20	DR1	DIF (8 digit BCD)	0Ch	
21	DR1	VIF (Energy kWh)	06h	
22	DR1	Value LSB	27h	
23	DR1	Value (= 2850427)	04h	
24	DR1	Value	85h	
25	DR1	Value MSB	02h	
26	DR2	DIF (8 digit BCD)	0Ch	
27	DR2	VIF (Volume liter)	13h	
28	DR2	Value LSB	76h	
29	DR2	Value (= 703476)	34h	
30	DR2	Value	70h	
31	DR2	Value MSB	00h	
32	DR3	DIF (8 digit BCD, StorageNo 1)	4Ch	
33	DR3	VIF (Energy kWh)	06h	
34	DR3	Value LSB	19h	
35	DR3	Value (= 1445419)	54h	
36	DR3	Value	44h	
37	DR3	Value MSB	01h	
38	DR4	DIF (Data type G, StorageNo 1)	42h	
39	DR4	VIF (Date)	6Ch	
40	DR4	Value LSB	FFh	
41	DR4	Value MSB (= 31.12.2007)	0Ch	
42	DR5	DIF (6 digit BCD)	0Bh	
43	DR5	VIF (Volume flow l/h)	3Bh	
44	DR5	Value LSB	27h	
45	DR5	Value (= 127)	01h	
46	DR5	Value MSB	00h	

47	DR6	DIF (6 digit BCD)	0Bh	Application layer (APL)
48	DR6	VIF (Power 100 mW)	2Ah	
49	DR6	Value LSB	97h	
50	DR6	Value (= 3297)	32h	
51	DR6	Value MSB	00h	
52	DR7	DIF (4 digit BCD)	0Ah	
53	DR7	VIF (Flow Temp. 100 m°C)	5Ah	
54	DR7	Value LSB	43h	
55	DR7	Value MSB (= 443)	04h	
56	DR8	DIF (4 digit BCD)	0Ah	
57	DR8	VIF (Return Temp. 100 m°C)	5Eh	
58	DR8	Value LSB	51h	
59	DR8	Value MSB (= 251)	02h	
60	DR9	DIF (2 byte integer)	02h	
61	DR9	VIF (FD-Table)	FDh	
62	DR9	VIFE (error flag)	17h	
63	DR9	Value LSB	00h	
64	DR9	Value MSB (= 0)	00h	
65	Checksum		C8h	DLL
66	Stop	Stop byte	16h	

Heat Cost Allocator

Example for Heat cost allocator with RF-Adapter	
Medium	Heat cost allocation
Manufacturer	QDS
Serial number of Radiomodule	11223344
Serial number of Meter (HCA)	55667788
Version	85
Status (Low Power/Battery low)	4
current cunsumption value	1234 HCA units
set date	30.04.2007
consumption at set date	23456 HCA units
currente temperature at sensor	25 °C

AES Key according to FIPS 197 (LSB first):
= manu. spec. at least 8 bytes unique for each meter
= 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

AES CBC Initial Vector according to FIPS 197 (LSB first):
= M Field + A Field + 8 bytes Acces No
= 93 44 88 77 66 55 55 08 00 00 00 00 00 00 00 00

SND_NR (wM-Bus)

		OMS wM-Bus frame	Heat cost allocator example		
Byte No	Field Name	Content	Bytes [hex] plain	Bytes [hex] AES coded	
1	L Field	Length of data (46 bytes)	29h	29h	Linklayer (DLL)
2	C Field	44h in Normal mode	44h	44h	
3	M Field	Manufacturer code	93h	93h	
4	M Field	Manufacturer code	44h	44h	
5	A Field	Serial No LSB (BCD)	44h	44h	
6	A Field	Serial No (BCD)	33h	33h	
7	A Field	Serial No (BCD) (= 11223344)	22h	22h	
8	A Field	Serial No MSB (BCD)	11h	11h	
9	A Field	Version (or Generation number)	55h	55h	
10	A Field	Device type (Medium=HCA)	08h	08h	
11	CRC 1		6Ch	6Ch	
12	CRC 1		B1h	B1h	
13	CI Field	72h means 12 bytes header	72h	72h	Application layer (APL)
14	Meter-ID	Serial No LSB (BCD)	88h	88h	
15	Meter-ID	Serial No (BCD)	77h	77h	
16	Meter-ID	Serial No (BCD) (= 55667788)	66h	66h	
17	Meter-ID	Serial No MSB (BCD)	55h	55h	
18	Meter-Man.	Meter Manufacturer code	93h	93h	
19	Meter-Man.	Meter Manufacturer code	44h	44h	
20	Meter-Vers.	Version (or Generation number)	55h	55h	
21	Meter-Med.	Device type (Medium=HCA)	08h	08h	
22	Access No.	Transmission counter	00h	00h	
23	Status	M-Bus state contents errors and alerts	04h	04h	
24	Signature	NNNNCCHHb (1 encr. block)	00h	10h	
25	Signature	BA00MMMMb (unidir., AES)	00h	05h	
26	AES-Verify	Encryption verification	2Fh	00h	
27	AES-Verify	Encryption verification	2Fh	DFh	
28	DR1	DIF (6 digit BCD)	0Bh	E2h	
29	CRC 2		25h	27h	DLL
30	CRC 2		CCh	F9h	
31	DR1	VIF (HCA-units)	6Eh	A7h	AES-Encrypted Block 1 / Application layer (APL)
32	DR1	Value LSB	34h	82h	
33	DR1	Value (= 001234 HCA-Units)	12h	14h	
34	DR1	Value MSB	00h	6Dh	
35	DR2	DIF (Data type G, StorageNo 1)	42h	15h	
36	DR2	VIF (Date)	6Ch	13h	
37	DR2	Value LSB	FEh	58h	
38	DR2	Value MSB (= 30.04.2007)	04h	1Ch	
39	DR3	DIF (6 digit BCD, StorageNo 1)	4Bh	D2h	
40	DR3	VIF (HCA-units)	6Eh	F8h	
41	DR3	Value LSB	56h	3Fh	
42	DR3	Value (= 023456 HCA-Units)	34h	39h	
43	DR3	Value MSB	02h	04h	
44	DR4	DIF (1 Byte integer)	01h	01h	Plain / Application layer (APL)
45	DR4	VIF (Temperature at Heating)	5Bh	5Bh	
46	DR4	Value (= 25 Grad Celsius)	19h	19h	
47	CRC 3		11h	61h	DLL
48	CRC 3		9Ah	09h	

RSP_UD (M-Bus with Encryption)

Byte No	Field Name	Content	OMS M-Bus frame Bytes [hex] plain	HCA example Bytes [hex] AES coded	
1	Start	Start byte	68h	68h	Linklayer (DLL)
2	L Field	Length of data (32 bytes)	22h	22h	
3	L Field	Length of data (32 bytes)	22h	22h	
4	Start	Start byte	68h	68h	
5	C Field	Respond user data	08h	08h	
6	A-Field	Secondary addressing mode	FDh	FDh	
7	CI Field	72h means 12 bytes header	72h	72h	Application layer (APL)
8	Ident.Nr.	Serial No LSB (BCD)	88h	88h	
9	Ident.Nr.	Serial No (BCD)	77h	77h	
10	Ident.Nr.	Serial No (BCD) (=12345678)	66h	66h	
11	Ident.Nr.	Serial No MSB (BCD)	55h	55h	
12	Manufr	Manufacturer code	93h	93h	
13	Manufr	Manufacturer code	44h	44h	
14	Version	Version (or Generation number)	55h	55h	
15	Device type	Device type (Medium=HCA)	08h	08h	
16	Access No.	Transmission counter	00h	00h	
17	Status	M-Bus state contents errors and alerts	04h	04h	
18	Signature	NNNNCCHHb (1 encr. block)	00h	10h	
19	Signature	BA00MMMMb (AES)	00h	05h	
20	AES-Verify	Encryption verification	2Fh	00h	AES-Encrypted Block 1
21	AES-Verify	Encryption verification	2Fh	DFh	
22	DR1	DIF (6 digit BCD)	0Bh	E2h	
23	DR1	VIF (HCA-units)	6Eh	A7h	
24	DR1	Value LSB	34h	82h	
25	DR1	Value (= 001234 HCA-Units)	12h	14h	
26	DR1	Value MSB	00h	6Dh	
27	DR2	DIF (Data type G, StorageNo 1)	42h	15h	
28	DR2	VIF (Date)	6Ch	13h	
29	DR2	Value LSB	FEh	58h	
30	DR2	Value MSB (= 30.04.2007)	04h	1Ch	
31	DR3	DIF (6 digit BCD, StorageNo 1)	4Bh	D2h	
32	DR3	VIF (HCA-units)	6Eh	F8h	
33	DR3	Value LSB	56h	3Fh	
34	DR3	Value (= 023456 HCA-Units)	34h	39h	
35	DR3	Value MSB	02h	04h	
36	DR4	DIF (1 Byte integer)	01h	01h	Plain
37	DR4	VIF (Temperature at Heating)	5Bh	5Bh	
38	DR4	Value (= 25 Grad Celsius)	19h	19h	
39	Checksum		F0h	40h	DLL
40	Stop	Stop byte	16h	16h	

Electricity Meter

Electricity meter example	
Medium	Electricity
Manufacturer	EMH
Serial number	00955118
Version	1
SML serverID = Register 0.0.0	0000000000955118
Main energy counter	0,021 kWh
Fabrication number	0000955118
Power	76,7 W

AES Key According to FIPS 197 (LSB first):
= manu. spec. at least 8 bytes unique for each meter
= 77 69 72 6D 61 63 68 65 6E 4D 55 43 6B 69 65 73

AES CBC Initial Vector according to FIPS 197 (LSB first):
= M Field + A Field + 8 bytes Acces No
= A8 15 18 51 95 00 01 02 09 09 09 09 09 09 09 09

5

SND_NR (wM-Bus + SML-Protocol)

		OMS wM-Bus frame	electricity meter example		
Byte No	Field Name	Content	Bytes [hex] plain	Bytes [hex] AES coded	
1	L Field	Length of data (190 bytes)	BEh	BEh	Linklayer (DLL)
2	C Field	44h in Normal mode	44h	44h	
3	M Field	Manufacturer code	A8h	A8h	
4	M Field	Manufacturer code	15h	15h	
5	A Field	Serial No LSB (BCD)	18h	18h	
6	A Field	Serial No (BCD)	51h	51h	
7	A Field	Serial No (BCD) (=00955118)	95h	95h	
8	A Field	Serial No MSB (BCD)	00h	00h	
9	A Field	Version (or Generation number)	01h	01h	
10	A Field	Device type (Medium=Electricity)	02h	02h	
11	CRC 1		6Dh	6Dh	
12	CRC 1		41h	41h	
13	CI Field	7Fh means 6 bytes header + SML	7Fh	7Fh	
14	Access No.	Transmission counter	09h	09h	
15	Status	M-Bus state contents errors and alerts	00h	00h	
16	Signature	NNNNCCHHb (11 encr. blocks)	00h	B0h	
17	Signature	BA00MMMMb (bidir., RX on, AES)	C0h	C5h	

18	AES-Verify	Encryption verification	2Fh	75h	AES-Encrypted Block 1	
19	AES-Verify	Encryption verification	2Fh	96h		
20	SML T/L	SML_Message (sequence)	76h	7Ah		
21	SML T/L	transactionId (TL[1] + octet_string[6])	07h	10h		
22	SML data	transactionId (MSB)	00h	1Ah		
23	SML data	transactionId (= 000000000287h)	00h	0Ah		
24	SML data	transactionId	00h	5Bh		
25	SML data	transactionId	00h	7Fh		
26	SML data	transactionId	02h	70h		
27	SML data	transactionId (LSB)	87h	13h		
28	SML T/L	groupNo (TL[1] + uint[1])	62h	22h		
29	CRC 2		74h	13h	DLL	
30	CRC 2		D3h	B3h		
31	SML data	groupNo (= 0)	00h	18h		Application layer (APL)
32	SML T/L	abortOnError (TL[1] + uint[1])	62h	B9h		
33	SML data	abortOnError (= 0)	00h	0Bh		
34	SML T/L	messageBody (choice)	72h	8Eh		
35	SML T/L	messageBody (TL[1] + uint[2])	63h	99h		
36	SML data	messageBody (MSB)	07h	8Eh	AES-Encrypted Block 2	
37	SML data	messageBody (LSB, = 0701h)	01h	7Dh		
38	SML T/L	SML_GetList_Res (sequence)	77h	79h		
39	SML T/L	clientId (not set)	01h	07h		
40	SML T/L	serverId (TL)	81h	4Ah		
41	SML T/L	serverId (TL[2] + octet_string[16])	02h	16h		
42	SML data	serverId (MSB)	30h	B5h		
43	SML data	serverId (= "0000000000955118")	30h	91h		
44	SML data	serverId	30h	07h		
45	SML data	serverId	30h	9Ah		
46	SML data	serverId	30h	CBh		
47	CRC 3		7Ch	69h	DLL	
48	CRC 3		06h	B8h		
49	SML data	serverId	30h	A3h		
50	SML data	serverId	30h	32h		
51	SML data	serverId	30h	A1h		
52	SML data	serverId	30h	39h		
53	SML data	serverId	30h	0Eh		
54	SML data	serverId	39h	BDh	AES-Encrypted Block 3	
55	SML data	serverId	35h	80h		
56	SML data	serverId	35h	9Ch		
57	SML data	serverId	31h	7Eh		
58	SML data	serverId	31h	60h		
59	SML data	serverId (LSB)	38h	99h		
60	SML T/L	listName (not set)	01h	27h		
61	SML T/L	actSensorTime (choice)	72h	5Ch		
62	SML T/L	actSensorTime (TL[1] + uint[1])	62h	B4h		
63	SML data	actSensorTime (= 1)	01h	C4h		
64	SML T/L	secIndex (TL[1] + uint[4])	65h	80h		
65	CRC 4		AFh	A3h	DLL	
66	CRC 4		2Dh	30h		
67	SML data	secIndex (MSB)	00h	D0h		
68	SML data	secIndex (= 383)	00h	0Ah		
69	SML data	secIndex	01h	CEh		
70	SML data	secIndex (LSB)	7Fh	19h		
71	SML T/L	valList (sequenceOf)	75h	03h		

72	SML T/L	valListEntry (sequence)	77h	C2h	AES-Encrypted Block 4
73	SML T/L	objName (TL[1] + octet_string[6])	07h	4Ch	
74	SML data	objName (MSB)	81h	F0h	
75	SML data	objName (= 8181C78203FFh)	81h	05h	
76	SML data	objName (= 129-129:199.130.03*255)	C7h	A5h	
77	SML data	objName	82h	86h	
78	SML data	objName	03h	54h	
79	SML data	objName (LSB)	FFh	4Bh	
80	SML T/L	status (not set)	01h	16h	
81	SML T/L	valTime (not set)	01h	98h	
82	SML T/L	unit (not set)	01h	11h	
83	CRC 5		A7h	5Eh	DLL
84	CRC 5		D6h	4Bh	
85	SML T/L	scaler (not set)	01h	EEh	
86	SML T/L	value (TL[1] + octet_string[3])	04h	0Ch	
87	SML data	value (MSB)	45h	C9h	
88	SML data	value (= "EMH")	4Dh	7Dh	
89	SML data	value (LSB)	48h	A2h	
90	SML T/L	valueSignature (not set)	01h	87h	AES-Encrypted Block 5
91	SML T/L	valListEntry (sequence)	77h	CAh	
92	SML T/L	objName (TL[1] + octet_string[6])	07h	4Ah	
93	SML data	objName (MSB)	01h	48h	
94	SML data	objName (= 0100000000FFh)	00h	E4h	
95	SML data	objName (= 1-0:0.0.0*255)	00h	1Fh	
96	SML data	objName	00h	C4h	
97	SML data	objName	00h	87h	
98	SML data	objName (LSB)	FFh	77h	
99	SML T/L	status (not set)	01h	2Eh	
100	SML T/L	valTime (not set)	01h	8Ah	
101	CRC 6		3Dh	E8h	DLL
102	CRC 6		9Eh	E3h	
103	SML T/L	unit (not set)	01h	30h	
104	SML T/L	scaler (not set)	01h	BDh	
105	SML T/L	value (TL)	81h	78h	
106	SML T/L	value (TL[2] + octet_string[16])	02h	57h	
107	SML data	value (MSB)	30h	8Ch	
108	SML data	value (= "0000000000955118")	30h	A4h	AES-Encrypted Block 6
109	SML data	value	30h	9Ah	
110	SML data	value	30h	39h	
111	SML data	value	30h	6Fh	
112	SML data	value	30h	28h	
113	SML data	value	30h	05h	
114	SML data	value	30h	56h	
115	SML data	value	30h	4Dh	
116	SML data	value	30h	9Eh	
117	SML data	value	39h	C5h	
118	SML data	value	35h	53h	
119	CRC 7		CBh	3Eh	DLL
120	CRC 7		EEh	76h	
121	SML data	value	35h	4Ch	
122	SML data	value	31h	53h	
123	SML data	value	31h	EEh	
124	SML data	value (LSB)	38h	AFh	
125	SML T/L	valueSignature (not set)	01h	0Ch	

126	SML T/L	valListEntry (sequence)	77h	EFh	AES-Encrypted Block 7
127	SML T/L	objName (TL[1] + octet_string[6])	07h	26h	
128	SML data	objName (MSB)	01h	1Ch	
129	SML data	objName (= 0100010801FFh)	00h	7Eh	
130	SML data	objName (= 1-0:1.8.1*255)	01h	BDh	
131	SML data	objName	08h	30h	
132	SML data	objName	01h	23h	
133	SML data	objName (LSB)	FFh	F0h	
134	SML T/L	status (TL[1] + uint[1])	62h	A3h	
135	SML data	status (= 128)	80h	F6h	
136	SML T/L	valTime (not set)	01h	52h	
137	CRC 8		59h	05h	DLL
138	CRC 8		A0h	0Fh	
139	SML T/L	unit (TL[1] + uint[1])	62h	1Ah	
140	SML data	unit (= 30)	1Eh	F4h	
141	SML T/L	scaler (TL[1] + sint[1])	52h	99h	
142	SML data	scaler (= -1)	FFh	A6h	
143	SML T/L	value (TL[1] + sint[5])	56h	FFh	
144	SML data	value (MSB)	00h	3Ch	AES-Encrypted Block 8
145	SML data	value (= 21)	00h	CCh	
146	SML data	value (= 0.021 kWh)	00h	6Bh	
147	SML data	value	00h	8Ch	
148	SML data	value (LSB)	15h	4Bh	
149	SML T/L	valueSignature (not set)	01h	9Ah	
150	SML T/L	valListEntry (sequence)	77h	8Bh	
151	SML T/L	objName (TL[1] + octet_string[6])	07h	F1h	
152	SML data	objName (MSB)	00h	0Ch	
153	SML data	objName (= 00006001FFh)	00h	C7h	
154	SML data	objName (= 0-0:C.1.255*255)	60h	D9h	
155	CRC 9		BAh	2Ah	DLL
156	CRC 9		C0h	F3h	
157	SML data	objName	01h	F6h	
158	SML data	objName	FFh	0Eh	
159	SML data	objName (LSB)	FFh	A9h	
160	SML T/L	status (not set)	01h	98h	
161	SML T/L	valTime (not set)	01h	89h	
162	SML T/L	unit (not set)	01h	A1h	AES-Encrypted Block 9
163	SML T/L	scaler (not set)	01h	84h	
164	SML T/L	value (TL[1] + octet_string[10])	0Bh	39h	
165	SML data	value (MSB)	30h	94h	
166	SML data	value (= "0000955118")	30h	D4h	
167	SML data	value	30h	C9h	
168	SML data	value	30h	24h	
169	SML data	value	39h	CAh	
170	SML data	value	35h	A5h	
171	SML data	value	35h	B2h	
172	SML data	value	31h	D7h	
173	CRC 10		88h	35h	DLL
174	CRC 10		2Fh	0Bh	
175	SML data	value	31h	ADh	
176	SML data	value (LSB)	38h	93h	
177	SML T/L	valueSignature (not set)	01h	A2h	
178	SML T/L	valListEntry (sequence)	77h	AAh	
179	SML T/L	objName (TL[1] + octet_string[6])	07h	58h	

180	SML data	objName (MSB)	01h	E7h	AES-Encrypted Block 10
181	SML data	objName (= 0100010700FFh)	00h	95h	
182	SML data	objName (= 1-0:1.7.0*255)	01h	48h	
183	SML data	objName	07h	92h	
184	SML data	objName	00h	9Ah	
185	SML data	objName (LSB)	FFh	92h	
186	SML T/L	status (not set)	01h	80h	
187	SML T/L	valTime (not set)	01h	C6h	
188	SML T/L	unit (TL[1] + uint[1])	62h	6Bh	
189	SML data	unit (= 27)	1Bh	AEh	
190	SML T/L	scaler (TL[1] + sint[1])	52h	35h	
191	CRC 11		EBh	3Fh	DLL
192	CRC 11		DAh	9Fh	
193	SML data	scaler (= -1)	FFh	91h	AES-Encrypted Block 11
194	SML T/L	value (TL[1] + sint[4])	55h	69h	
195	SML data	value (MSB)	00h	EFh	
196	SML data	value (= 767)	00h	E8h	
197	SML data	value (= 76.7 W)	02h	20h	
198	SML data	value (LSB)	FFh	D9h	
199	SML T/L	valueSignature (not set)	01h	07h	
200	SML T/L	listSignature (not set)	01h	56h	
201	SML T/L	actGatewayTime (not set)	01h	48h	
202	SML T/L	crc16 (TL[1] + uint[2])	63h	8Dh	
203	SML data	crc16 (MSB)	D1h	62h	
204	SML data	crc16 (= D12Ch)	2Ch	C4h	
205	SML T/L	endOfSmlMsg	00h	1Ch	
206	Dummy	Fill Byte due to AES	2Fh	91h	
207	Dummy	Fill Byte due to AES	2Fh	D0h	
208	Dummy	Fill Byte due to AES	2Fh	AFh	
209	CRC 12		2Ah	6Eh	DLL
210	CRC 12		BAh	0Eh	
211	Dummy	Fill Byte due to AES	2Fh	84h	
212	Dummy	Fill Byte due to AES	2Fh	E9h	
213	Dummy	Fill Byte due to AES	2Fh	32h	
214	Dummy	Fill Byte due to AES	2Fh	65h	
215	Dummy	Fill Byte due to AES	2Fh	66h	
216	CRC 13		25h	66h	DLL
217	CRC 13		EEh	A9h	

RSP_UD (M-Bus + SML-Protocol)

Byte No		OMS M-Bus frame	electricity meter	
	Field Name	Content	Bytes [hex]	
			plain	
1	Start	Start byte	68h	Linklayer (DLL)
2	L Field	Length of data (183 bytes)	B7h	
3	L Field	Length of data (183 bytes)	B7h	
4	Start	Start byte	68h	
5	C Field	Respond user data	08h	
6	A-Field	Secondary addressing mode	FDh	
7	CI Field	7Eh means 14 bytes header + SML	7Eh	Application layer (APL)
8	Ident.Nr.	Serial No LSB (BCD)	18h	
9	Ident.Nr.	Serial No (BCD)	51h	
10	Ident.Nr.	Serial No (BCD) (=00955118)	95h	
11	Ident.Nr.	Serial No MSB (BCD)	00h	
12	Manufr	Manufacturer code	A8h	
13	Manufr	Manufacturer code	15h	
14	Version	Version (or Generation number)	01h	
15	Device type	Device type (Medium=Electricity)	02h	
16	Access No.	Transmission counter	09h	
17	Status	M-Bus state contents errors and alerts	00h	
18	Signature	no Encryption	00h	
19	Signature	no Encryption	00h	
20	AES-Verify	Encryption verification	2Fh	
21	AES-Verify	Encryption verification	2Fh	
22	SML T/L	SML_Message (sequence)	76h	
23	SML T/L	transactionId (TL[1] + octet_string[6])	07h	
24	SML data	transactionId (MSB)	00h	
25	SML data	transactionId (= 000000000287h)	00h	
26	SML data	transactionId	00h	
27	SML data	transactionId	00h	
28	SML data	transactionId	02h	
29	SML data	transactionId (LSB)	87h	
30	SML T/L	groupNo (TL[1] + uint[1])	62h	
31	SML data	groupNo (= 0)	00h	
32	SML T/L	abortOnError (TL[1] + uint[1])	62h	
33	SML data	abortOnError (= 0)	00h	
34	SML T/L	messageBody (choice)	72h	
35	SML T/L	messageBody (TL[1] + uint[2])	63h	
36	SML data	messageBody (MSB)	07h	
37	SML data	messageBody (LSB, = 0701h)	01h	

38	SML T/L	SML_GetList_Res (sequence)	77h	Application layer (APL)
39	SML T/L	clientId (not set)	01h	
40	SML T/L	serverId (TL)	81h	
41	SML T/L	serverId (TL[2] + octet_string[16])	02h	
42	SML data	serverId (MSB)	30h	
43	SML data	serverId (= "0000000000955118")	30h	
44	SML data	serverId	30h	
45	SML data	serverId	30h	
46	SML data	serverId	30h	
47	SML data	serverId	30h	
48	SML data	serverId	30h	
49	SML data	serverId	30h	
50	SML data	serverId	30h	
51	SML data	serverId	30h	
52	SML data	serverId	39h	
53	SML data	serverId	35h	
54	SML data	serverId	35h	
55	SML data	serverId	31h	
56	SML data	serverId	31h	
57	SML data	serverId (LSB)	38h	
58	SML T/L	listName (not set)	01h	
59	SML T/L	actSensorTime (choice)	72h	
60	SML T/L	actSensorTime (TL[1] + uint[1])	62h	
61	SML data	actSensorTime (= 1)	01h	
62	SML T/L	secIndex (TL[1] + uint[4])	65h	
63	SML data	secIndex (MSB)	00h	
64	SML data	secIndex (= 383)	00h	
65	SML data	secIndex	01h	
66	SML data	secIndex (LSB)	7Fh	
67	SML T/L	valList (sequenceOf)	75h	
68	SML T/L	valListEntry (sequence)	77h	
69	SML T/L	objName (TL[1] + octet_string[6])	07h	
70	SML data	objName (MSB)	81h	
71	SML data	objName (= 8181C78203FFh)	81h	
72	SML data	objName (= 129-129:199.130.03*255)	C7h	
73	SML data	objName	82h	
74	SML data	objName	03h	
75	SML data	objName (LSB)	FFh	
76	SML T/L	status (not set)	01h	
77	SML T/L	valTime (not set)	01h	
78	SML T/L	unit (not set)	01h	
79	SML T/L	scaler (not set)	01h	
80	SML T/L	value (TL[1] + octet_string[3])	04h	
81	SML data	value (MSB)	45h	
82	SML data	value (= "EMH")	4Dh	
83	SML data	value (LSB)	48h	
84	SML T/L	valueSignature (not set)	01h	
85	SML T/L	valListEntry (sequence)	77h	
86	SML T/L	objName (TL[1] + octet_string[6])	07h	
87	SML data	objName (MSB)	01h	
88	SML data	objName (= 0100000000FFh)	00h	
89	SML data	objName (= 1-0:0.0.0*255)	00h	
90	SML data	objName	00h	
91	SML data	objName	00h	
92	SML data	objName (LSB)	FFh	

93	SML T/L	status (not set)	01h	Application layer (APL)
94	SML T/L	valTime (not set)	01h	
95	SML T/L	unit (not set)	01h	
96	SML T/L	scaler (not set)	01h	
97	SML T/L	value (TL)	81h	
98	SML T/L	value (TL[2] + octet_string[16])	02h	
99	SML data	value (MSB)	30h	
100	SML data	value (= "0000000000955118")	30h	
101	SML data	value	30h	
102	SML data	value	30h	
103	SML data	value	30h	
104	SML data	value	30h	
105	SML data	value	30h	
106	SML data	value	30h	
107	SML data	value	30h	
108	SML data	value	30h	
109	SML data	value	39h	
110	SML data	value	35h	
111	SML data	value	35h	
112	SML data	value	31h	
113	SML data	value	31h	
114	SML data	value (LSB)	38h	
115	SML T/L	valueSignature (not set)	01h	
116	SML T/L	valListEntry (sequence)	77h	
117	SML T/L	objName (TL[1] + octet_string[6])	07h	
118	SML data	objName (MSB)	01h	
119	SML data	objName (= 0100010801FFh)	00h	
120	SML data	objName (= 1-0:1.8.1*255)	01h	
121	SML data	objName	08h	
122	SML data	objName	01h	
123	SML data	objName (LSB)	FFh	
124	SML T/L	status (TL[1] + uint[1])	62h	
125	SML data	status (= 128)	80h	
126	SML T/L	valTime (not set)	01h	
127	SML T/L	unit (TL[1] + uint[1])	62h	
128	SML data	unit (= 30)	1Eh	
129	SML T/L	scaler (TL[1] + sint[1])	52h	
130	SML data	scaler (= -1)	FFh	
131	SML T/L	value (TL[1] + sint[5])	56h	
132	SML data	value (MSB)	00h	
133	SML data	value (= 21)	00h	
134	SML data	value (= 0.021 kWh)	00h	
135	SML data	value	00h	
136	SML data	value (LSB)	15h	
137	SML T/L	valueSignature (not set)	01h	
138	SML T/L	valListEntry (sequence)	77h	
139	SML T/L	objName (TL[1] + octet_string[6])	07h	
140	SML data	objName (MSB)	00h	
141	SML data	objName (= 00006001FFh)	00h	
142	SML data	objName (= 0-0:C.1.255*255)	60h	
143	SML data	objName	01h	
144	SML data	objName	FFh	
145	SML data	objName (LSB)	FFh	

146	SML T/L	status (not set)	01h	Application layer (APL)
147	SML T/L	valTime (not set)	01h	
148	SML T/L	unit (not set)	01h	
149	SML T/L	scaler (not set)	01h	
150	SML T/L	value (TL[1] + octet_string[10])	0Bh	
151	SML data	value (MSB)	30h	
152	SML data	value (= "0000955118")	30h	
153	SML data	value	30h	
154	SML data	value	30h	
155	SML data	value	39h	
156	SML data	value	35h	
157	SML data	value	35h	
158	SML data	value	31h	
159	SML data	value	31h	
160	SML data	value (LSB)	38h	
161	SML T/L	valueSignature (not set)	01h	
162	SML T/L	valListEntry (sequence)	77h	
163	SML T/L	objName (TL[1] + octet_string[6])	07h	
164	SML data	objName (MSB)	01h	
165	SML data	objName (= 0100010700FFh)	00h	
166	SML data	objName (= 1-0:1.7.0*255)	01h	
167	SML data	objName	07h	
168	SML data	objName	00h	
169	SML data	objName (LSB)	FFh	
170	SML T/L	status (not set)	01h	
171	SML T/L	valTime (not set)	01h	
172	SML T/L	unit (TL[1] + uint[1])	62h	
173	SML data	unit (= 27)	1Bh	
174	SML T/L	scaler (TL[1] + sint[1])	52h	
175	SML data	scaler (= -1)	FFh	
176	SML T/L	value (TL[1] + sint[4])	55h	
177	SML data	value (MSB)	00h	
178	SML data	value (= 767)	00h	
179	SML data	value (= 76.7 W)	02h	
180	SML data	value (LSB)	FFh	
181	SML T/L	valueSignature (not set)	01h	
182	SML T/L	listSignature (not set)	01h	
183	SML T/L	actGatewayTime (not set)	01h	
184	SML T/L	crc16 (TL[1] + uint[2])	63h	
185	SML data	crc16 (MSB)	D1h	
186	SML data	crc16 (= D12Ch)	2Ch	
187	SML T/L	endOfSmlMsg	00h	
188	Checksum		09h	DLL
189	Stop	Stop byte	16h	

Installation Procedure with a Special Installation Telegram

MUC example	
Medium(MUC)	System
Manufacturer	OMS
Serial number	33445566
Version	10 (e.g. V 1.0)

Gas meter example	
Medium	Gas
Manufacturer	ELS
Serial number	12345678
Version	51 (e.g. V 5.1)
Model/Version	BKG4
Hardware Version	15 (e.g. V 1.5)
Metrology Firmware Version	11 (e.g. V 1.1)
Other Software Version	10 (e.g. V 1.0)
Metering Point ID	DE 123456 49074
	00000000000012345678

AES Key According to FIPS 197 (LSB first):
= manu. spec. at least 8 bytes unique for each meter
= 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 11

AES CBC Initial Vector according to FIPS 197 (LSB first):
= M Field + A Field + 8 bytes Acces No
= 93 15 78 56 34 12 33 03 01 01 01 01 01 01 01 01

SND-IR (wM-Bus - short address)

		OMS wM-Bus frame	Gas meter -> MUC		
Byte No	Field Name	Content	Bytes [hex]	Bytes [hex]	
			plain	AES coded	
1	L Field	Length of data (78 bytes)	4Eh	4Eh	Linklayer (DLL)
2	C Field	46h in Installation Mode	46h	46h	
3	M Field	Manufacturer code	93h	93h	
4	M Field	Manufacturer code	15h	15h	
5	A Field	Serial No LSB (BCD)	78h	78h	
6	A Field	Serial No (BCD)	56h	56h	
7	A Field	Serial No (BCD) (=12345678)	34h	34h	
8	A Field	Serial No MSB (BCD)	12h	12h	
9	A Field	Version (or Generation number)	33h	33h	
10	A Field	Device type (Medium=Gas)	03h	03h	
11	CRC 1		52h	53h	
12	CRC 1		2Eh	2Eh	
13	CI Field	7Ah means 4 bytes header	7Ah	7Ah	AES-Encrypted Block 1
14	Access No.	Transmission counter	01h	01h	
15	Status	M-Bus state contents errors and alerts	00h	00h	
16	Signature	NNNNCCHHb (3 encr. blocks, static tlg.)	08h	38h	
17	Signature	BA00MMMMb (bidir., RX off, AES)	80h	85h	
18	AES-Verify	Encryption verification	2Fh	C8h	
19	AES-Verify	Encryption verification	2Fh	51h	
20	DR1	DIF (Variable length)	0Dh	9Ch	
21	DR1	VIF (Extension)	FDh	92h	
22	DR1	VIFE (Version)	0Ch	ABh	
23	DR1	LVAR (= 4 byte text string)	04h	D2h	
24	DR1	Value (LSB)	34h	F3h	
25	DR1	Value (= BKG4)	47h	B2h	
26	DR1	Value	4Bh	DFh	
27	DR1	Value (MSB)	42h	1Fh	
28	DR2	DIF (16-bit Integer/Binary)	02h	63h	
29	CRC 2		40h	01h	DLL
30	CRC 2		41h	38h	
31	DR2	VIF (Extension)	FDh	87h	
32	DR2	VIFE (Hardware version)	0Dh	30h	
33	DR2	Value LSB (=1.5)	05h	2Ch	
34	DR2	Value MSB	01h	5Ah	
35	DR3	DIF (16-bit Integer/Binary)	02h	23h	

36	DR3	VIF (Extension)	FDh	A7h	AES-Encrypted Block 2	Application layer (APL)
37	DR3	VIFE (Metrology Firmware version)	0Eh	6Ah		
38	DR3	Value LSB (= 1.1)	01h	1Fh		
39	DR3	Value MSB	01h	96h		
40	DR4	DIF (16-bit Integer/Binary)	02h	29h		
41	DR4	VIF (Extension)	FDh	CBh		
42	DR4	VIFE (Other firmware version)	0Fh	65h		
43	DR4	Value LSB (= 1.0)	00h	64h		
44	DR4	Value MSB	01h	8Ah		
45	DR5	DIF (Variable length)	0Dh	3Eh		
46	DR5	VIF (Extension)	FDh	A5h		
47	CRC 3		0Dh	B1h	DLL	
48	CRC 3		BEh	9Bh		
49	DR5	VIFE (customer location)	10h	A9h		Application layer (APL)
50	DR5	LVAR (=33 byte text string)	21h	31h		
51	DR5	Value LSB	38h	54h		
52	DR5	Value (= 00000000000012345678)	37h	3Eh		
53	DR5	Value	36h	9Eh		
54	DR5	Value	35h	C8h	AES-Encrypted Block 3	
55	DR5	Value	34h	4Dh		
56	DR5	Value	33h	37h		
57	DR5	Value	32h	6Eh		
58	DR5	Value	31h	80h		
59	DR5	Value	30h	9Ch		
60	DR5	Value	30h	C6h		
61	DR5	Value	30h	CEh		
62	DR5	Value	30h	C7h		
63	DR5	Value	30h	3Ch		
64	DR5	Value	30h	B9h		
65	CRC 4		02h	ECh	DLL	
66	CRC 4		34h	B1h		
67	DR5	Value	30h	91h		Application layer (APL)
68	DR5	Value	30h	68h		
69	DR5	Value	30h	4Eh		
70	DR5	Value	30h	B3h		
71	DR5	Value	30h	B3h		
72	DR5	Value	30h	21h	AES-Encrypted Block 4	
73	DR5	Value (= 49074)	34h	BFh		
74	DR5	Value	37h	39h		
75	DR5	Value	30h	FBh		
76	DR5	Value	39h	F6h		
77	DR5	Value	34h	7Eh		
78	DR5	Value (= 123456)	36h	64h		
79	DR5	Value	35h	4Fh		
80	DR5	Value	34h	4Fh		
81	DR5	Value	33h	EAh		
82	DR5	Value	32h	A0h		
83	CRC 5		1Dh	3Ah	DLL	
84	CRC 5		01h	2Eh		
85	DR5	Value	31h	EFh		
86	DR5	Value (= DE)	45h	AAh		
87	DR5	Value MSB	44h	D8h		
88	Dummy	Fill Byte due to AES	2Fh	58h		
89	Dummy	Fill Byte due to AES	2Fh	12h		
90	CRC 6		4Fh	98h	DLL	
91	CRC 6		F2h	3Eh		

CNF-IR (wM-Bus)

Byte No	Field Name	OMS wM-Bus frame Content	MUC -> Gas meter Bytes [hex] plain	Bytes [hex] AES coded	
1	L Field	Length of data (22 bytes)	16h	16h	Linklayer (DLL)
2	C Field	06h in Installation Mode	06h	06h	
3	M Field	Manufacturer code	B3h	B3h	
4	M Field	Manufacturer code	3Dh	3Dh	
5	A Field	Serial No LSB (BCD)	66h	66h	
6	A Field	Serial No (BCD)	55h	55h	
7	A Field	Serial No (BCD) (=33445566)	44h	44h	
8	A Field	Serial No MSB (BCD)	33h	33h	
9	A Field	Version (or Generation number)	0Ah	0Ah	
10	A Field	Device type (Medium=MUC)	31h	31h	
11	CRC 1		9Dh	9Dh	
12	CRC 1		AEh	AEh	
13	CI Field	80h means 12 byte header	80h	80h	Application layer (APL)
14	Ident.Nr.	Serial No LSB (BCD)	78h	78h	
15	Ident.Nr.	Serial No (BCD)	56h	56h	
16	Ident.Nr.	Serial No (BCD) (=12345678)	34h	34h	
17	Ident.Nr.	Serial No MSB (BCD)	12h	12h	
18	Manufr	Manufacturer code	93h	93h	
19	Manufr	Manufacturer code	15h	15h	
20	Version	Version (or Generation number)	33h	33h	
21	Device type	Device type (Medium=Gas)	03h	03h	
22	Access No.	Transmission counter	01h	01h	
23	Status	MUC state cont. recept. level (-80dBm)	19h	19h	
24	Signature	NNNNCCHHb	00h	00h	
25	Signature	BA00MMMMb (bidir., RX on, no encr.)	C0h	C0h	
26	CRC 2		14h	14h	DLL
27	CRC 2		97h	97h	

Send a Command with an Acknowledge

A SNE_UD is applied to transport a command to a meter or actuator. When C-field 53h or 73h is applied the meter will acknowledge a successful reception of the command. The bit “application error” in the status byte of the meter’s acknowledge indicates that an application error has happened during command execution.

MUC example	
Medium/device type	OMS MUC
Manufacturer	HYD
Serial number	90123456
Version	8

water meter with RF adapter example	
Medium/device type	Water
Manufacturer	HYD
Serial number water meter	92752244
Serial number RF adapter	43886102
Version	41

AES Key According to FIPS 197 (LSB first):
= manu. spec. at least 8 bytes unique for each meter
= 82 B0 55 11 91 F5 1D 66 EF CD AB 89 67 45 23 01

AES CBC Initial Vector according to FIPS 197 (LSB first):
= M Field + A Field + 8 bytes Acces No
= 24 23 44 22 75 92 29 07 7D 7D 7D 7D 7D 7D 7D 7D

SND-UD; Correction of time (wM-Bus)

		OMS wM-Bus frame	MUC -> water meter		
Byte No	Field Name	Content	Bytes [hex]	Bytes [hex]	
			plain	AES coded	
1	L Field	Length of data (38 bytes)	26h	26h	Linklayer (DLL)
2	C Field	Send user data	53h	53h	
3	M Field	Manufacturer code	24h	24h	
4	M Field	Manufacturer code	23h	23h	
5	A Field	Serial No LSB (BCD)	56h	56h	
6	A Field	Serial No (BCD)	34h	34h	
7	A Field	Serial No (BCD)	12h	12h	
8	A Field	Serial No MSB (BCD) of MUC	90h	90h	
9	A Field	Version (or Generation number)	08h	08h	
10	A Field	Device type (OMS MUC)	31h	31h	
11	CRC 1		CBh	CBh	
12	CRC 1		8Eh	8Eh	
13	CI Field	Special CI to add/subtract time offset	6Dh	6Dh	Application Layer
14	Ident.Nr.	Serial No LSB (BCD)	44h	44h	
15	Ident.Nr.	Serial No (BCD)	22h	22h	
16	Ident.Nr.	Serial No (BCD)	75h	75h	
17	Ident.Nr.	Serial No MSB (BCD) of meter	92h	92h	
18	Manufr	Manufacturer code	24h	24h	
19	Manufr	Manufacturer code	23h	23h	
20	Version	Version (or Generation number)	29h	29h	
21	Device type	Device type (Medium = Water)	07h	07h	
22	Access No.	Transmission counter	7Dh	7Dh	
23	Status	MUC state (no RSSI level available)	00h	00h	
24	Signature	NNNNCCHHb (1 encr. block)	00h	10h	
25	Signature	BA00MMMMb (bidir., RX on, AES)	C0h	05h	
26	AES-Verify	Encryption verification	2Fh	3Ah	
27	AES-Verify	Encryption verification	2Fh	97h	
28	TC-Field	Add time difference	01h	31h	
29	CRC 2		77h	14h	DLL
30	CRC 2		61h	25h	
31	Time	Value format J, LSB	32h	FBh	AES Encrypted Block 1
32	Time	Value (add 1 minute, 50 seconds)	01h	F4h	
33	Time	Value MSB	00h	34h	
34	Reserved	Reserved, set to 0	00h	68h	
35	Reserved	Reserved, set to 0	00h	1Ch	
36	Reserved	Reserved, set to 0	00h	41h	
37	Reserved	Reserved, set to 0	00h	54h	
38	Reserved	Reserved, set to 0	00h	78h	
39	Reserved	Reserved, set to 0	00h	FBh	
40	CMD-Verify	Command verification	2Fh	EAh	
41	CMD-Verify	Command verification	2Fh	0Bh	
42	CMD-Verify	Command verification	2Fh	C6h	
43	CMD-Verify	Command verification	2Fh	6Eh	
44	CRC 3		79h	A0h	DLL
45	CRC 3		F1h	27h	

ACK (wM-Bus - long Address)

		OMS wM-Bus frame	water meter -> MUC		
Byte No	Field Name	Content	Bytes [hex] plain	Bytes [hex] AES coded	
1	L Field	Length of data (22 bytes)	16h	16h	Linklayer (DLL)
2	C Field	Acknowledge	00h	00h	
3	M Field	Manufacturer code	24h	24h	
4	M Field	Manufacturer code	23h	23h	
5	A Field	Serial No LSB (BCD)	02h	02h	
6	A Field	Serial No (BCD)	61h	61h	
7	A Field	Serial No (BCD)	88h	88h	
8	A Field	Serial No MSB (BCD) of RF-Adapter	43h	43h	
9	A Field	Version (or Generation number)	29h	29h	
10	A Field	Device type (Medium=Water)	07h	07h	
11	CRC 1		34h	34h	
12	CRC 1		87h	87h	
13	CI Field	8Bh means 12 byte header	8Bh	8Bh	Application layer (APL)
14	Ident.Nr.	Serial No LSB (BCD)	44h	44h	
15	Ident.Nr.	Serial No (BCD)	22h	22h	
16	Ident.Nr.	Serial No (BCD)	75h	75h	
17	Ident.Nr.	Serial No MSB (BCD) of meter	92h	92h	
18	Manufr	Manufacturer code	24h	24h	
19	Manufr	Manufacturer code	23h	23h	
20	Version	Version (or Generation number)	29h	29h	
21	Device type	Device type (Medium=Water)	07h	07h	
22	Access No.	Transmission counter	7Dh	7Dh	
23	Status	M-Bus state contents errors and alerts	00h	00h	
24	Signature	NNNNCCHHb	00h	00h	
25	Signature	BA00MMMMb (bidir, RX off)	80h	80h	
26	CRC 2		EFh	EFh	DLL
27	CRC 2		D5h	D5h	

Request of the Selected Data

A REQ_UD2 is used either to request the standard meter consumption data or to read responses of a command or prove successful execution of a command. After a command the RSP_UD may consist of either the expected answer to that command (e.g. “get valve state”) or the standard answer if the command “set new key” was applied or an “application error” if the execution of the command was not successful (e.g. using the wrong encryption key for this meter). An application error will be indicated in the status byte of the meter’s acknowledge telegram.

Example for MUC	
Medium	MUC
Manufacturer	TCH
Serial number	66778899
Version	12
Status (no error)	0
Meter-RSSI	-84 dBm

Example for Heat cost allocator	
Medium	Heat Cost Allocatior
Manufacturer	TCH
Serial number	12345678
Version	143
Status (no error)	0
current cunsumption value	12345 HCA units
due date	31.12.2009
consumption at due date	23456 HCA units

AES Key According to FIPS 197 (LSB first):
= manu. spec. at least 8 bytes unique for each meter
= 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

AES CBC Initial Vector according to FIPS 197 (LSB first):
= M Field + A Field + 8 bytes Acces No
= 68 50 78 56 34 12 8F 08 02 02 02 02 02 02 02 02

REQ_UD2 (wM-Bus)

		OMS wM-Bus frame	MUC -> HCA		
Byte No	Field Name	Content	Bytes [hex] plain	Bytes [hex] AES coded	
1	L Field	Length of data (22 bytes)	16h	16h	Linklayer (DLL)
2	C Field	Request user data class 2 (5Bh or 7Bh)	5Bh	5Bh	
3	M Field	Manufacturer code	68h	68h	
4	M Field	Manufacturer code	50h	50h	
5	A Field	Serial No LSB (BCD)	99h	99h	
6	A Field	Serial No (BCD)	88h	88h	
7	A Field	Serial No (BCD) (=66778899)	77h	77h	
8	A Field	Serial No MSB (BCD) of MUC	66h	66h	
9	A Field	Version (or Generation number)	0Ch	0Ch	
10	A Field	Device type (Medium=MUC)	31h	31h	
11	CRC 1		29h	29h	
12	CRC 1		80h	80h	
13	CI Field	MUC -> Meter	80h	80h	Application layer (APL)
14	Ident.Nr.	Meter-ID	78h	78h	
15	Ident.Nr.	Meter-ID	56h	56h	
16	Ident.Nr.	Meter-ID	34h	34h	
17	Ident.Nr.	Meter-ID	12h	12h	
18	Manufr	Meter-Manufacturer-ID	68h	68h	
19	Manufr	Meter-Manufacturer-ID	50h	50h	
20	Version	Meter-Version	8Fh	8Fh	
21	Device type	Meter-Device-Type	08h	08h	
22	Access No.	Transmission counter	02h	02h	
23	Status	MUC State RSSI level (-84dBm)	17h	17h	
24	Signature	NNNNCCHHb	00h	00h	
25	Signature	BA00MMMMb, (bidir., RX on, no encr.)	C0h	C0h	
26	CRC 2		ABh	ABh	DLL
27	CRC 2		85h	85h	

RSP-UD (wM-Bus - short address)

		OMS wM-Bus frame	HCA -> MUC		
Byte No	Field Name	Content	Bytes [hex] plain	Bytes [hex] AES coded	
1	L Field	Length of data (30 bytes)	1Eh	1Eh	Linklayer (DLL)
2	C Field	Respond user data	08h	08h	
3	M Field	Manufacturer code	68h	68h	
4	M Field	Manufacturer code	50h	50h	
5	A Field	Serial No LSB (BCD)	78h	78h	
6	A Field	Serial No (BCD)	56h	56h	
7	A Field	Serial No (BCD) (=12345678)	34h	34h	
8	A Field	Serial No MSB (BCD) of meter	12h	12h	
9	A Field	Version (or Generation number)	8Fh	8Fh	
10	A Field	Device type (Medium=HCA)	08h	08h	
11	CRC 1		99h	99h	
12	CRC 1		38h	38h	

13	CI Field	7Ah means 4 bytes header	7Ah	7Ah	APL
14	Access No.	Transmission counter	02h	02h	
15	Status	M-Bus state contains errors and alerts	00h	00h	
16	Signature	NNNNCCHHb (1 encr. block)	10h	10h	
17	Signature	BA00MMMMb, (bidir.,RX off; AES)	85h	85h	
18	AES-Verify	Encryption verification	2Fh	FDh	AES-Encrypted Block 1
19	AES-Verify	Encryption verification	2Fh	26h	
20	DR1	DIF (24 bit binary, StorageNo 0)	03h	EFh	
21	DR1	VIF (HCA-units)	6Eh	68h	
22	DR1	Value LSB	39h	ACh	
23	DR1	Value (= 012345d = 003039h HCA-Units)	30h	F6h	
24	DR1	Value MSB	00h	5Bh	
25	DR2	DIF (16 bit binary, StorageNo 1)	42h	AEh	
26	DR2	VIF (Date type G)	6Ch	02h	
27	DR2	Value LSB	3Fh	8Bh	
28	DR2	Value MSB (= 31.12.2009)	1Ch	FDh	Application layer
29	CRC 2		75h	44h	DLL
30	CRC 2		5Dh	CAh	
31	DR3	DIF (24 bit binary, StorageNo 1)	43h	C1h	
32	DR3	VIF (HCA-units)	6Eh	88h	
33	DR3	Value LSB	A0h	D8h	
34	DR3	Value (= 023456 = 005BA0h HCA-Units)	5Bh	A9h	
35	DR3	Value MSB	00h	72h	
36	CRC 3		23h	F4h	DLL
37	CRC 3		5Ch	77h	

or alternative..

RSP_UD (wM-Bus - Appl. Error)

		OMS wM-Bus frame	HCA -> MUC		
Byte No	Field Name	Content	Bytes [hex]	Bytes [hex]	
			plain	AES coded	
1	L Field	Length of data (11 bytes)	0Bh	0Bh	Linklayer (DLL)
2	C Field	Respond user data	08h	08h	
3	M Field	Manufacturer code	68h	68h	
4	M Field	Manufacturer code	50h	50h	
5	A Field	Serial No LSB (BCD)	78h	78h	
6	A Field	Serial No (BCD)	56h	56h	
7	A Field	Serial No (BCD) (=12345678)	34h	34h	
8	A Field	Serial No MSB (BCD)	12h	12h	
9	A Field	Version (or Generation number)	8Fh	8Fh	
10	A Field	Device type (Medium=HCA)	08h	08h	
11	CRC 1		B2h	B2h	
12	CRC 1		78h	78h	
13	CI Field	Application Error	70h	70h	APL
14	Error	Application error code	14h	14h	
15	CRC 2		46h	46h	DLL
16	CRC 2		56h	56h	

This example shows an “application error”, which is responded instead of expected data because the MUC applied a wrong key in the encrypted command.

Reset of the Link by a SND-NKE

If the MUC intend to finish communication it sends a SND-NKE as last. The meter/actuator responds to this SND-NKE with an ACK. After that the repetition of the last send telegram stops.

MUC example	
Medium(MUC)	System
Manufacturer	OMS
Serial number	66778899
Version	12
Meter-RSSI	-66 dBm
Access number	03

Example for cooling meter	
Medium	cool_outlet
Manufacturer	QDS
Serial number of Heatmeter	11223344
Version	16
Status (no error)	0

SND-NKE (wM-Bus)

		OMS wM-Bus frame	MUC -> cooling meter		
Byte No	Field Name	Content	Bytes [hex]	Bytes [hex]	
			plain	AES coded	
1	L Field	Length of data (22 bytes)	16h	16h	Linklayer (DLL)
2	C Field	Request user data class 2 (5Bh or 7Bh)	5Bh	5Bh	
3	M Field	Manufacturer code	68h	68h	
4	M Field	Manufacturer code	50h	50h	
5	A Field	Serial No LSB (BCD)	99h	99h	
6	A Field	Serial No (BCD)	88h	88h	
7	A Field	Serial No (BCD) (=66778899)	77h	77h	
8	A Field	Serial No MSB (BCD) of MUC	66h	66h	
9	A Field	Version (or Generation number)	0Ch	0Ch	
10	A Field	Device type (Medium=MUC)	31h	31h	
11	CRC 1		29	29	
12	CRC 1		80	80	
13	CI Field	MUC -> Meter (long header)	80h	80h	Application layer (APL)
14	Ident.Nr.	Serial No LSB (BCD)	44	88h	
15	Ident.Nr.	Serial No (BCD)	33	77h	
16	Ident.Nr.	Serial No (BCD) (=12345678)	22	66h	
17	Ident.Nr.	Serial No MSB (BCD)	11	55h	
18	Manufr	Manufacturer code	93h	93h	
19	Manufr	Manufacturer code	44h	44h	
20	Version	Version (or Generation number)	10h	10h	
21	Device type	Device type (Medium=Cool_outlet)	0Ah	0Ah	
22	Access No.	Transmission counter	03h	03h	
23	Status	MUC State RSSI level (-66dBm)	20h	20h	
24	Signature	NNNNCCHHb	00h	00h	
25	Signature	BA00MMMMb, (bidir., RX on, no encr.)	C0h	C0h	
26	CRC 2		1E	BD	DLL
27	CRC 2		80	B6	

ACK (wM-Bus- short Address)

Byte No	Field Name	Content	OMS wM-Bus frame cooling meter -> MUC Bytes [hex] plain	Bytes [hex] AES coded	
1	L Field	Length of data (14 bytes)	0Eh	0Eh	Linklayer (DLL)
2	C Field	Acknowledge	00h	00h	
3	M Field	Manufacturer code	93h	24h	
4	M Field	Manufacturer code	44h	23h	
5	A Field	Serial No LSB (BCD)	44h	02h	
6	A Field	Serial No (BCD)	33h	61h	
7	A Field	Serial No (BCD)	22h	88h	
8	A Field	Serial No MSB (BCD) of RF-Adapter	11h	43h	
9	A Field	Version (or Generation number)	10h	10h	
10	A Field	Device type (Medium=Cool_Outlet)	0Ah	0Ah	
11	CRC 1		55	AF	
12	CRC 1		93	60	
13	CI Field	Meter->MUC (short header)	8Ah	8Ah	APL
14	Access No.	Transmission counter	03h	03h	
15	Status	M-Bus state contents errors and alerts	00h	00h	
16	Signature	NNNNCCHHb	00h	00h	
17	Signature	BA00MMMMb (bidir, RX off)	80h	80h	
18	CRC 2		BC	BC	DLL
19	CRC 2		5E	5E	