Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie BSI TR-03109-1

Anlage III: Feinspezifikation „Drahtlose LMN-Schnittstelle“
Teil a: „OMS Specification Volume 2, Primary Communication“

Version 1.0, Datum 18.03.2013

Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-100

E-Mail: smartmeter@bsi.bund.de
Internet: https://www.bsi.bund.de

Einleitung

Dieses Dokument ist Teil der Anlage III zur Technischen Richtlinie BSI TR-03109-1 „Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems“. Diese Anlage basiert auf den folgenden beiden Dokumenten:

- OMS Specification Volume 2, Primary Communication, Issue 3.0.1
- OMS Technical Report Security, Issue 1.1.0

Die „OMS Specification Volume 2“ spezifiziert in der vorliegenden Version alle funktionalen Anforderungen der EN-13757 näher aus, so dass Geräte, die der Norm sowie der Spezifikation unterliegen, untereinander interoperabel sind. Die funktionalen Anforderungen decken somit auch Funktionen ab, die bei der Umsetzung in einem Smart Meter Gateway nach Schutzprofil und Technischer Richtlinie an der dafür vorgesehenen LMN-Schnittstelle explizit ausgeschlossen (bspw. Zeit-Synchronisation, Unterbrecher-Vorrichtungen) bzw. eingeschränkt (bspw. kryptographische Primitiven) sind.

Die in der Technischen Richtlinie TR-03109-3 definierten kryptographischen Anforderungen für die drahtlose LMN-Schnittstellen sind im „OMS Technical Report Security“ beschrieben und ersetzen somit die Vorgaben aus der „OMS Specification Volume 2“.

Die Technische Richtlinie BSI TR-03109-1 macht in Kapitel 3.3 Vorgaben, wie die beiden Dokumente anzuwenden sind, sowie welche kryptographischen Primitiven auf dieser Schnittstelle zum Smart Meter Gateway zulässig sind. Im Zweifelsfalle gelten die Vorgaben aus den Technischen Richtlinien.

Open Metering System Specification

Volume 2
Primary Communication

Issue 3.0.1 / 2011-01-29

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	Formatting and Proposals	T. Blank
0.9.5	2008-06-12	Results of Karlsruhe 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 adoptions; table index added; content index limited to structure level 3.	H. Baden
1.0.3	2009-02-25	Correct mistake in Table 10 Add changes for 2nd Version	U. Pahl
1.0.4	2009-05-13	Revision in AG1	AG1
1.0.5	2009-05-30	Add changes for 2nd Version	U. Pahl
1.0.6	2009-06-11	Update Annex	U. Pahl
1.0.7	2009-06-30	Changes based on protocol#23	U. Pahl
1.0.8	2009-07-03	Last changes of online review; update Annex A;,L and M, editorial review	U. Pahl
1.0.8	2009-07-05	Editorial and formal review	H. Baden
1.0.9	2009-07-17	Add Time sync frame to MUC-Status, separate ACC-No for M-Bus and wM-Bus	U. Pahl
2.0.0	2009-07-20	Release as V2.0.0	U. Pahl
2.0.1	2010-04-10	Add Changes for 3rd Version, Add sync Meter transmission; New CI-Fields	U. Pahl
2.0.2	2010-11-05	Add Compact M-Bus Profile; Harmonise Spec. with prEN 13757-3/4	U. Pahl
2.0.3	2010-11-17	Revision in AG1	AG1
2.0.4	2010-12-17	Comments from members of AG1, Bug fix in Annex B	U. Pahl
3.0.0	2011-01-21	Update Changes from Standard revision	U. Pahl
3.0.1	2011-01-28	Editorial Revision. Release as V3.0.1	U. Pahl / A. Bolder

Table of contents

List of tables

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 and abbreviations 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” describe mandatory requirements. Statements with a “should” describe recommendations.

This part concentrates on the requirements for basic meters but also includes some optional enhancements for sophisticated meters. This 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 NTA 8130.

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

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

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 [EN 13757-2]. 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 100 mA (42 V / 420 Ω), and reduces the energy converted into heat in the bus interface. For the requirements for wiring and installation refer to [EN 13757-2]

2.2 Wireless Communication (wM-Bus)

2.2.1 Modes and Requirements

The [EN 13757-4] (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 [EN 13757-4] 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 [EN 13757-5] covering such relaying via meters does not apply to the proposed modes S and T.

As for the various modes described in [EN 13757-4], 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 – 870 MHz license free frequency range. The duty cycle does not limit the functions required for the Open Metering System but limits the band occupation time from other systems operating in these frequency bands.

Note that the total average transmit duty cycle per hour is limited by the [EN 13757-4] for the S1-mode to 0.02 %, corresponding to a total transmit time of not more than 720 ms 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 [ERC 7003], 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 [EN 13757-4] 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 [EN 13757-4]. 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 2.

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 Configuration 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 [REC 7003] there is a minimum time delay between successive transmissions of 1.8 s for the S-modes and 0.72 s for the T-Modes.

Therefore a bidirectional meter/actuator (both S- or T-Mode) shall delay every response or acknowledge to the MUC at least for 2 seconds after the reception of a request or command.

2.2.2.1 Synchronous versus asynchronous transmission

In order to enable battery efficient communication partners (data concentrators, repeaters …) that only switch on their receivers for predicted short time windows, the meter shall follow a strict transmission time scheme. A transmission regarding this time scheme is called synchronous transmission. It is based on a nominal transmission time point and an additional scatter.

The next nominal transmission time point is given by the last nominal transmission time point and the nominal transmission interval. The scatter is the deviation from the nominal transmission time point.

The next individual transmission time point is calculated by the last transmission time point and the individual transmission interval for next transmission (n+1) based on the access number:

$$t_{TX}(n+1) = t_{TX}(n) + T_{ACC}(n+1)$$

with

$$T_{ACC}(n+1) = (1 + (|ACC - 128| - 64) / 2048) \times T_{nom}$$

$$T_{nom} = N \times 2 \text{ seconds}$$

where

- $t_{TX}(n+1)$ is next synchronous transmission time point
- $t_{TX}(n)$ is last synchronous transmission time point
- $T_{ACC}(n+1)$is the interval from the synchronous transmission with the access number ACC to the next synchronous transmission,
- ACC is the value of the access number (0 … 255),
- T_{nom} is the fixed nominal interval which is freely chosen with N multiple of 2 seconds, observing the limits given by Table 1. Duty cycle constraints need to be observed, as well.
- N is a fixed unsigned integer factor larger than 1

Table 1 — Limits of the nominal transmission interval

Mode	Maximum of nominal transmission interval [min]
S-Mode	90
T-Mode	15

The access number ACC shall be incremented and put to modulus 256 after every synchronous transmission and never else. (Refer to chapter 2.2.3)

The nominal interval T_{nom} shall be accurate with a tolerance of

- +110/-30 ppm for meters operating in the temperature range -15 … +65 ℃ or
- +230/-30 ppm for all other meters.

An additional non-accumulative jitter on the transmission interval T_{ACC} due to discrete time quantization is allowed. This jitter shall be less than ±1 ms for $T_{nom} < 300$ seconds and ±3 ms otherwise.

All synchronous transmissions shall be marked as such by setting the Bit S in the Configuration Word (refer to Table 14).

The meter/actuator may also send additional telegrams in the meanwhile of the synchronous transmissions (e.g. installation telegrams, responses to the MUC or additional SND-NR). All transmission happens outside the synchronous time scheme are called asynchronous transmission. Asynchronous transmissions shall never change the access number. They are marked with a clear Bit S in the Configuration Word (refer to Table 14).

The synchronous transmission shall be one of the message types SND-NR, ACC-DMD or ACC-NR (refer to Table 6). If the nominal transmission interval is smaller than the selected update interval of consumption data (refer to Table 2) then one or several ACC-NR may be used for synchronous transmission between the synchronous transmissions of the SND-NR. The ratio of ACC-NR versus SND-NR (respectively ACC-DMD in case of alert) shall be n/1 to allow a reception of every n^{th} telegram only (with n = 0 … 15) by a battery operated receiver. The ratio shall not be changed after the installation of the meter/actuator.

The meter may omit single synchronous transmissions if a task of higher priority (e.g. a metrological algorithm that cannot be postponed) needs to be performed at the scheduled transmission time point. The rate of omitted synchronous messages shall not exceed 6.25 % per sliding 24 h time period. The Access Number shall be incremented as if all synchronous transmissions had been executed.

The start of the first synchronous transmission shall be stochastic. It is not allowed to fix the synchronous transmission exactly to a common event like a special time or a power on after a central voltage drop. This is required to avoid a concurrent use of the radio channel by many meters. Refer also to chapter 4.2.2.1.

An example in Annex M shows the prediction of a synchronous transmission.

2.2.2.2 Interval of consumption data

An update of consumption data with every synchronous transmission is recommended. However the consumption data shall be updated at least with the average update interval maximum as listed in Table 2 plus additional scatter.

See the following table for the mandatory data update periods:

Table 2 — Update interval of consumption data for different media

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

Table 2 shows data visualization intervals for informative and billing aspects. For consumers, the visualization intervals for different media are 15 respectively 60 minutes at a typical reception probability of more than 95 %. Informative intervals are given to provide actual data for consumers.

2.2.2.3 Interval of installation data

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

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

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 12).

2.2.2.4 Interval of management data

If the meter/actuator provides special management data (static data only, no consumption data or other time variant data) then it shall mark this as a static telegram (refer to Table 12) and send it at least twice a day.

2.2.3 Access Timing of a Meter or Actuator

A meter/actuator signals its own accessibility in the Configuration Word (encryption mode 0, 5 and 6 only) of every transmission (refer to Configuration Word in Table 14). The meter/actuator initiates periodical transmissions. If the MUC wants to transmit a telegram to a meter dedicated to him it checks in the Configuration Word if the meter is accessible.

Table 3 — Accessibility of a meter/actuator

Conf. Bit 15 (B)	Conf. Bit 14 (A)	Accessibility of a meter/actuator
0	0	Meter/actuator provides no access windows (unidirectional meter)
0	1	Meter/actuator supports bidirectional access in general, but there is no access window after this transmission (e.g. temporarily no access in order to keep duty cycle limits or to limit energy consumption)
1	0	Meter/actuator provides a short access windows only immediately after this transmission (e.g. battery operated meter)
1	1	Meter/actuator provides unlimited access at least until the next transmission (e.g. mains powered devices)

Unidirectional meters (modes S1 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 [EN 13757-4] and depends on the mode. The referred standard defines for S2-mode a response time t_{RO} and for T2-mode an acknowledge delay t_{ACK} after transmission (refer to Table 4).

The response time t_{RO} respective acknowledge delay t_{ACK} (as defined in [EN 13757-4]) 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 preamble as described in [EN 13757-4] 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 (FAC). During the Frequent Access Cycle, the meter/actuator shall repeat the last message periodically with a FAC-Transmission delay t_{TxD} (refer to Table 4) until the next request/command is received (or time out). The FAC-Transmission delay shall not be changed during the Frequent Access Cycle. This allows the MUC or other communication device a fast access to the meter/actuator even in case of a lost message. The Frequent Access Cycle lasts until t_{TO} (refer to Table 4) counted from 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 (refer to Table 5). The access timing is shown in Annex L.

Table 4 — Timing parameter for meter access

Parameter	Sym	Min	Type	Max	Unit	Note
S2-Response delay (MUC to meter)	t_{RO}	3		50	ms	
T2-Response delay (MUC to meter)	t_{ACK}	2		3	ms	
FAC Transmission delay [a b c]	t_{TxD}	N × 1000 - 0,5	N × 1000	N × 1000 + 0,5	ms	N = 2, 3, 4 or 5
FAC Time out [d]	t_{TO}	25		30	s	

[a] FAC Transmission delay: describes the duration which a meter shall delay the first response to a received message from the MUC referred to its last transmission. This delay shall also be applied between the first response of the meter and the next repeated response of the meter and all following repeated responses during the Frequent Access Cycle (FAC). The reference time point shall be the end of the preamble (end of the sync sequence) of the meter transmission.

[b] The selected timeslot N shall be the same throughout the Frequent Access Cycle.

[c] The tolerance is related to the last transmission in the FAC. If several transmissions were missed then the accumulated tolerance has to be considered.

[d] FAC Time out: is the time period between the last successful reception of a frame from the MUC during the Frequent Access Cycle (FAC) and the moment where the repetition of the last response of the meter shall be stopped (end of Frequent Access Cycle).

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 Configuration Word (Bit B=0; A=1; refer to Table 3) 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 Configuration Word of the next transmission (Bit B = 1).

2.3 Power Line Communication

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 [EN 13757-2]. The selection of a meter by secondary address (refer to [EN 13757-3] chapter 11.3) and the support of wild cards for wild card search (refer to [EN 13757-3] chapter 11.5) shall be supported. Additionally the support of extended selection method (selection via fabrication number) is also required (refer to [EN 13757-3] chapter 11.4). If a meter uses encrypted data transfer then the fabrication number shall be transmitted in the unencrypted area.

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

3.2 Wireless Communication (wM-Bus)

The link layer is fully described in [EN 13757-4]. Annex C and D of that standard contain telegram examples together with an application layer according to [EN 13757-3] (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 and an one byte device type identification. Note that the byte version is not restricted in use as software version. It may apply also for other address purposes like coding of the manufacture location as long as grant a worldwide unique addressing of this meter. 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 N 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 (e.g. using an external radio adapter), it has to be applied in the application layer using the Long 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 [EN 60870-5-2].

There are different message types for data exchange:

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

The message type is signalled by the C-field.

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

Table 5 — C-fields of master (MUC or other communication device)

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[2]	Send command (Send User Data)	ACK
REQ-UD1	5Ah[2], 7Ah[2]	Alarm request , (Request User Data Class1)	ACK, RSP_UD
REQ-UD2	5Bh[2], 7Bh[2]	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	-

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:

Table 6 — C-fields of slave (meter or actuator)

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-NR	47h	No data - provides the opportunity to access the meter, between two application data transmissions.	-
ACC-DMD	48h	Access demand to master in order to request new important application data (alerts)	ACK
ACK	00h[2], 10h[2], 20h[2], 30h[2]	Acknowledge the reception of a SND-UD (acknowledgement of transmission only); It shall also be used as a response to an REQ-UD1, when no alert happened	-
RSP-UD	08h[2], 18h[2], 28h[2], 38h[2]	Response of application data after a request from master (response of user data)	-

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

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

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 Transport Layer (Short or Long Header) as described in the [EN 13757-4] are used for all application layers. The structure of this header and the following application layer is defined by the CI-field. For all other message types without application data the header conforms to the new applied CI-field pure Transport layer (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 chapter4.2.2). 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 2). 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 10) 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 Configuration 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

A fully functional bidirectional repeater will be defined in a separate volume of the OMS 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 [EN 13757-3]. It may transport either the meter application layer according to [EN 13757-3] (M-Bus), or alternatively [EN 13757-1] (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: 5

Table 7 — List of supported CI-fields

CI-field	Direction	Header length	Application protocol
50h	Application select to device	None	M-Bus (for wired M-Bus only!)
51h	CMD to device	None	M-Bus (for wired M-Bus only!)
52h	Selection of device	None	M-Bus (for wired M-Bus only!)
5Ah	CMD to device	4 Bytes	M-Bus [a] (not used for wireless M-Bus now)
5Bh	CMD to device	12 Bytes	M-Bus [a]
60h	CMD to device	14 Bytes	DLMS [a, b]
61h	CMD to device	6 Bytes	DLMS [a, b] (not used for wireless M-Bus now)
64h	CMD to device	14 Bytes	SML [a, b]
65h	CMD to device	6 Bytes	SML [a, b] (not used for wireless M-Bus now)
6Ch	Time Sync to device	14 Byte	Generic
6Dh	Time Sync to device	14 Byte	Generic
6Eh	Error from device	4 Bytes	Generic
6Fh	Error from device	12 Bytes	Generic
70h	Error from device	None	Generic (for wired M-Bus only!)
71h	Alarm from device	None	Generic (for wired M-Bus only!)
72h	Response from device	12 Bytes	M-Bus
74h	Alarm from device	4 Bytes	Generic
75h	Alarm from device	12 Bytes	Generic
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 [a, b]
7Dh	Response from device	6 Bytes	DLMS [a, b]
7Eh	Response from device	14 Bytes	SML [a, b]
7Fh	Response from device	6 Bytes	SML [a, b]
80h	Transport layer to device	12 Byte	None [a]
8Ah	Transport layer from device	4 Bytes	None [a]
8Bh	Transport layer from device	12 Bytes	None [a]

[a] This CI-Fields are planned in a revision of the [EN 13757-3] (CI-values reserved so far)

[b] Refer also [EN 13757-1], [EN 62056-61], [DLMS-UA] or [SML-spec]:

The application layer standards are:

- M-Bus: [EN 13757-3]
- DLMS: [EN 13757-1], [EN 62056-61], [DLMS-UA]
- SML, [SML-spec]

The header structures are:

- 4 bytes: As for CI = 7Ah of [EN 13757-3],
  If the telegram contains such a "short" header the meter identification is taken from the link layer,
- 12 bytes: As for CI = 72h of [EN 13757-3],
  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 other application protocols (e.g. SML or DLMS) 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 Short/Long Header for wM-Bus has to contain at least:

- Access number
- Status byte
- Configuration 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. It will be distinguished between:

- Meter access number
- MUC access number

The meter access number is generated by a meter/actuator. It shall be incremented by 1 (and only 1) with every synchronous transmission (refer to chapter 2.2.2.1). Asynchronous transmissions shall always apply the access number of the last synchronous transmission. The meter access number shall be applied to SND-NR, SNR-IR, ACC-NR and ACC-DMD telegrams. If a MUC accepts an ACC-DMD or an SND-IR from a meter/actuator it has to send an acknowledgement (ACK or CNF-IR) using the received meter access number. The received MUC access number has no impact on the stored meter access number of the meter/actuator. After power up of the meter its value of the access number shall be set by a randomized initial value from 0 to 255. The access number of the meter shall not be resettable.

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 [EN 13757-3].

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 6Eh, 6Fh, 72h, 74h, 75h, 7Ah, 7Ch, 7Dh, 7Eh, 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:

Table 8 — MUC status field reception level

Bit #	Value
0 … 5	Received RSSI value for a reception level in range of -128 … -6 dBm Reception level is calculated by -130 dBm + 2 × RSSI-Value (1 … 62) If RSSI value = 0 no reception level is available If RSSI value = 63 the reception level is > -6 dBm
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 MUC. 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 [EN 13757-3] (2004). The usage of these bits is explained in Table 9.

Table 9 — Use of bits in the Meter status byte

Bit #	Value for Single Error (Hex)	Name according to EN 13757-3
0	00h 01h	No error Application busy
1	02h 03h	Any application error Abnormal condition / alarm
2	04h	Low Power
3	08h	Permanent error
4	10h	Temporary error
5	20h	Specific to manufacturer
6	40h	Specific to manufacturer
7	80h	Specific to manufacturer

The Status byte may have more than one error bit set at any time.

No error — is the default value and used if no error happened.

Application busy — shall be used when the Application is too busy to provide requested data in time.

Any application error shall be used to communicate a failure during the interpretation or the execution of a received command, e.g. if a not decryptable telegram was received. The application errors are listed in Annex E.

Abnormal conditions shall be used if a correct working application detects an abnormal behaviour like a permanent flow of water by a water meter.

Low Power Warning - The bit “Power low” is set only to signal interruption of Power supply or end of battery life (which requires a service action during the next 15 month).

Permanent error Failure - The bit “permanent error” is set only if the meter signals a fatal device error (which requires a service action). Error can be reset only by a service action.

Temporary error Warning – The bit “temporary error” is set only if the meter signals an error condition (which not immediately requires maintenance). This error condition may later disappear.

Specific to manufact. These bits are used manufacturer specific. A set bit may signal an error or another state.

The status field allows an application layer-response within an "ACK" telegram (note that this telegram only confirms the telegram-reception). In this way, "any application error" shall be used to communicate a failure during the interpretation or the execution of a received command. Note that more detailed error description may be provided by an application error telegram starting with CI = 6Eh, 6Fh or 70h when a REQ-UD2 is applied after an "any application error".

Details about other error conditions like "permanent error" may be provided in application protocol (refer to chapter 5.1.2).

4.2.4 Supported Device Types (Medium)

For the Open Metering System several meter device types shall be supported at minimum (refer to foot note of Table 10).

Table 10 listed both device types from Table 3 of [EN13757-3] (2004) as well as new declared device types. It is recommended to support all device types as listed in this table.

Table 10 — List of device types (with extension of Table 3 in [EN 13757-3] (2004))

Device type (previously called medium)	**Code bin. Bit 7 … 0**	**Code hex.**
Other	0000 0000	00
Oil	0000 0001	01
Electricity [d]	0000 0010	02
Gas [d]	0000 0011	03
Heat [d]	0000 0100	04
Steam	0000 0101	05
Warm Water (30 °C … 90 °C) [d]	0000 0110	06
Water [d]	0000 0111	07
Heat Cost Allocator [d]	0000 1000	08
Compressed Air	0000 1001	09
Cooling load meter (Volume measured at return temperature: outlet) [d]	0000 1010	0A
Cooling load meter (Volume measured at flow temperature: inlet) [d]	0000 1011	0B
Heat (Volume measured at flow temperature: inlet) [d]	0000 1100	0C
Heat / Cooling load meter [d]	0000 1101	OD
Bus / System component	0000 1110	0E
Unknown Medium	0000 1111	0F
Reserved for utility meter	…	10 to 13
Calorific value	0001 0100	14
Hot water (≥ 90 °C)	0001 0101	15
Cold water	0001 0110	16
Dual register (hot/cold) Water meter [a]	0001 0111	17
Pressure	0001 1000	18
A/D Converter	0001 1001	19
Smoke detector	0001 1010	1A
Room sensor (e.g. temperature or humidity)	0001 1011	1B
Gas detector	0001 1100	1C
Reserved for sensors	…	1D to 1F
Breaker (electricity) [d]	0010 0000	20

Table 10 – continued

Device type (previously called medium)	Code bin. Bit 7 … 0	Code hex.
Valve (gas) [d]	0010 0001	21
Reserved for switching devices	…	22 to 24
Customer unit (Display device)	0010 0101	25
Reserved for customer units	…	26 to 27
Waste water	0010 1000	28
Garbage	0010 1001	29
Carbon dioxide	0010 1010	2A
Reserved for environmental meter	…	2B to 2F
Reserved for system devices	…	30
OMS MUC [d]	0011 0001	31
OMS unidirectional repeater [d]	0011 0010	32
OMS bidirectional repeater [e]	0011 0011	33
Reserved for system devices	…	34 to 35
Radio converter (System side) [b, d]	0011 0110	36
Radio converter (Meter side) [c, d]	0011 0111	37
Reserved for system devices	…	38 to 3F
Reserved	…	40 to FF

a Such a meter registers water flow above a limit temperature in a separate register with an appropriate tariff ID.

b A Radio converter at System side operates as Radio master like a MUC

c A Radio converter at Meter side operates as Radio slave like a RF-Meter

d These Device types shall be supported by the MUC!

e Note that this device type will is in preparation and will be mandatory in a future revision.

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 header after the CI-field, are never encrypted. The encryption mode does not use the obsolete DES modes 2 or 3 as suggested in [EN 13757-3] (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 Configuration Word (referred to as encryption methods in [EN 13757-3] (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 14)
- 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):

Table 11 — Initialisation vector for the CBC-AES-128

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

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 or a counter 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. Note that after 255 transmissions the zero consumption is detectable again even if the access number was used. The access number will be incremented with each synchronous transmission only.

[3] 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!

Therefore it is recommended to add a time stamp or a sequence number (VIFE "Unique telegram identification (previously named 'Access Number (transmission count)')") to the telegram content.

4.2.5.4 Configuration Word (Encryption Mode and Communication Status Bits)

The Configuration 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 14). For the communication on wired M-Bus all bits in the Configuration Word except “MMMM” and “NNNN” should be set to “0”.

The coding of the Configuration Word 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.

Table 12 — Contents of meter telegram (from the meter/actuator to the MUC)

Conf. Bit 3	Conf. 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 13 — Contents of MUC authentication (from the MUC to the meter/actuator)

Conf. Bit 3	Conf. 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.

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

The Bits A and B of the Configuration Word are used for access control to the meter /actuator as described in chapter 2.2.3. The Bit S of the Configuration Word is used for a synchronous transmission as described in chapter 2.2.2.1. Thus, the complete Configuration Word is:

Table 14 — Definition of the Configuration Word for encryption modes MMMM = 5 or 6

MS Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	LS Bit 0
bidirectional communication	accessibility	synchronous	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	S	0	M	M	M	M	N	N	N	N	C	C	H	H

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 Configuration 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 Configuration Word as well. For other application protocols than M-Bus these 2 bytes are a part of the Short or Long Header.

4.2.5.6 Examples

Annex N 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:

Table 15 — Required value resolution with power/flow data

Medium	**Billing**	**Power / flow resolution**
Electricity	≤ 1 kWh	≤ 1 W
Water	≤ 1 m^3	No requirement
Gas $Q_{Max} \leq 6$ m^3/h	≤ 1 m^3	≤ 10 l/h
Gas $Q_{Max} \leq 60$ m^3/h	≤ 1 m^3	≤ 100 l/h
Gas $Q_{Max} > 60$ m^3/h	≤ 1 m^3	≤ 1000 l/h
Heat / Cold $Q_p < 10$ m^3/h	≤ 1 kWh	No requirement
Heat / Cold $Q_p < 100$ m^3/h	≤ 10 kWh	No requirement
Heat / Cold $Q_p \geq 100$ m^3/h	≤ 100 kWh	No requirement
Heat cost allocation	No requirement	No requirement

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.

Table 16 — Required value resolution without power/flow data

Medium	**Index resolution**
Electricity	≤ 0.1 Wh
Water	≤ 1 ^{3}
Gas $Q_{Max} \leq 6$ m^3/h	≤ 10 l
Gas $Q_{Max} \leq 60$ m^3/h	≤ 100 l
Gas $Q_{Max} > 60$ m^3/h	≤ 1000 l
Heat / Cold	No requirement
Heat cost allocation	No requirement

4.2.6.3 Required Time Information

If there is no power/flow information present, additional requirements for the accuracy and resolution of the actual time difference between the index values are to be considered 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 one transmission interval and if such delay of two adjacent transmissions varies by less than 1% of the nominal 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 adjacent transmission time points varies by more than 1% of the transmission interval or the delay is longer than one nominal transmission interval then each telegram shall contain sufficient time information to calculate this time difference. This time information shall be provided with the data point "actuality duration" signalling the actual time delay between time of meter reading and transmit time with a resolution of 1s.

4.2.6.3.3 Transmission on Request

In case of a transmission on request the meter must enable the MUC to calculate the consumption out of two adjacent transmissions. Therefore the meter has to follow a certain time scheme for the generation (and transmission) of its index values.
The reference time is the time point of the first request transmission (REQ_UD2) by the MUC or another communication unit.
The devices (meter, actuator) are allowed to generate the values with a fixed delay from the reference time. The delay should not vary by more than 1 second.

4.3 Generic Services

4.3.1 Clock Synchronisation

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

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

The Annex F describes the transmission of the clock synchronisation to the 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 [EN 13757-3] (2004).

5 Application Protocols

5.1 M-Bus Application Protocol

5.1.1 Supported Data Types (DIFs)

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 [EN 13757-3] (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) and its extension F0h to F4h 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 … 0F4h), thus allowing binary numbers of up to 32 bytes (256 bits). The new defined codes (0F0h … 0F4h) had been reserved so far. The usage for that LVAR extension shall be:

LVAR = F0h - F4h: Binary number with 4 × (LVAR - 0ECh) bytes (16, 20, 24, 28, 32) bytes

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 [EN 13757-3] (2004) shall be supported.

5.1.2 Supported Record Types (VIFs)

Measured values and units

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

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

For the required volume the VIFs E0010nnnb (1 ml to 10 m³) shall be used, whereas for the possibly required flow the VIFs E0111nnnb (1 ml/h to 10 m³/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. 0.001 ℃ to 1 ℃), E10111nnb (return temperature) or E11000nnb for temperature difference (1 mK to 1 K) shall be used,

All these values may use the VIF = 0FBh with the (combinable/orthogonal) VIF-extensions E1110nnnb (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. The date/time of storage number 0 mark the current date/time of the device. If the date/time of current value differs from current date/time (uncorrelated transmission – refer to chapter 4.2.6.3) then an additional delay ((“actuality duration”) is added. 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 the averaging time interval of power or flow values E11100nnb (“averaging duration”) shall be used.

For an uncorrelated transmission the elapsed time between measurement and transmission shall be coded as E11101nnb (“actuality duration” -1s to 1day).

The nominal transmission interval used for synchronous transmission should be declared in installation telegrams (if available) with E011 11nnb (“Period of nominal data transmissions” - seconds or minutes). It may also used in other types of telegrams.

Management data

For optional transmission of ownership number the VIF = 0FDh with VIF-extension E0010001b (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 E0010000b (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 E1110001b (so far reserved). The value is given in dBm.

Example: 01h FDh 71h A1h means -95 dBm (binary) and 0Ah FDh 71h 85h F0h means -85 dBm (BCD). If no value available the value should be set invalid like 01h FDh 71h 80h (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: 21h FDh 71h 9Ch 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: 31h FDh 71h 9Fh means a noise level of -97 dBm.

Else

Details about the error state indicated by status byte (refer to chapter 4.2.3.2) shall be coded with VIF = FDh and VIFE = E0010111b and optional with orthogonal VIFE = 00011100b. The meaning of this error code is either manufacturer specific or if this orthogonal VIFE applied based on Annex H of prEN 13757-3:2011. Example: 02h FDh 17h 04h 00h means error code 4.

If a sequence number is used it shall be coded with VIF = 0FDh and VIF extension E0001000b ("Unique telegram identification (previously named 'Access Number (transmission count)')"). Refer also to chapter 4.2.5.3. Example: 04h FDh 08h 34h 12h 00h 00h.

All other VIFs and DIFs of [EN 13757-3] 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 12). 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 [EN 13757-1].

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 N (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 0 ≤ 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.

Note that the time stamp "Time, date of reading" (A-0:0.1.2*255) is calculated by the MUC itself based on the time stamp "Date of device" (A-0:0.9.2*255) and "Time of device" (A-0:0.9.1*255) and the lapsed run time.

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 reading	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	
	–	kWh	10e-6 … 10e+1	0000 cccc			1000 0nnn	0011 1011		
	–	kWh	10e+2 … 10e+3	0000 cccc			1111 1011	1000 000n	0011 1011	
	–	kWh	10e+5 … 10e+6	0000 cccc			1111 1011	1000 000n	1111 1101	0011 1011
O	Meter reading	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	
	–	kWh	10e-6 … 10e+1	1x00 cccc	1000 xxxx	0000 00xx	1000 0nnn	0011 1011		
	–	kWh	10e+2 … 10e+3	1x00 cccc	1000 xxxx	0000 00xx	1111 1011	1000 000n	0011 1011	
	–	kWh	10e+5 … 10e+6	1x00 cccc	1000 xxxx	0000 00xx	1111 1011	1000 000n	1111 1101	0011 1011
A1	Meter reading	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 reading	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
A1	Meter reading	1-0:15.8.0*255	Active energy import (abs.(*A*)), current value							
	–	kWh	10e-6 … 10e+1	0000 cccc			1000 0nnn	1111 1100	0001 0000	
	–	kWh	10e+2 … 10e+3	0000 cccc			1111 1011	1000 000n	1111 1100	0001 0000
	–	kWh	10e+5 … 10e+6	0000 cccc			1111 1011	1000 000n	1111 1101	…
							… 1111 1100 0001 0000			
O	Meter reading	1-0:15.8.0*VZ	Active energy import (abs.(*A*)), recent value							
	–	kWh	10e-6 … 10e+1	1x00 cccc	1000 xxxx	0000 00xx	1000 0nnn	1111 1100	0001 0000	
	–	kWh	10e+2 … 10e+3	1x00 cccc	1000 xxxx	0000 00xx	1111 1011	1000 000n	1111 1100	0001 0000
	–	kWh	10e+5 … 10e+6	1x00 cccc	1000 xxxx	0000 00xx	1111 1011	1000 000n	1111 1101	…
							… 1111 1100 0001 0000			

O	Time of device	1-0:0.9.1*255	Current time at time of transmission				
	–	Type F		0000 0100			0110 1101
O	Date of device	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	Time, date of reading	1-0:0.1.2*255	Run time difference between measurement of current value and transmission				
				0000 cccc			0111 01nn
O	Date of reading	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 reading	4-0:1.0.0*255	Unrated integral, current value		
	–	HCA	10e+0	`0000 cccc`	`0110 1110`
M	Meter reading	4-0:1.2.0*255	Unrated integral, set date value		
	–	HCA	10e+0	`0100 cccc`	`0110 1110`
O	Time of device	4-0:0.9.1*255	Current time at time of transmission		
	–	Type F		`0000 0100`	`0110 1101`
O	Date of device	4-0:0.9.2*255	Current date at time of transmission		
	–	Type G		`0000 0010`	`0110 1100`
	–	Type F		`0000 0100`	`0110 1101`
O	Time, date of reading	4-0:0.1.2*255	Run time difference between measurement of current value and transmission		
				`0000 cccc`	`0111 01nn`
M	Date of reading	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 reading	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 reading	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	Meter reading	5-0:2.0.0*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 reading	5-0:2.2.0*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	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	Temperatur	5-0:10.0.0*255	Flow temperature, current value				
	–	℃	10e-3 … 10e+0	0000 cccc	0101 10nn		
O	Temperatur	5-0:11.0.0*255	Return temperature, current value				
	–	℃	10e-3 … 10e+0	0000 cccc	0101 11nn		

O	Time of device	5-0:0.9.1*255	Current time at time of transmission		
	–	Type F		0000 0100	0110 1101
O	Date of device	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	Time, date of reading	5-0:0.1.2*255	Run time difference between measurement of current value and transmission		
				0000 cccc	0111 01nn
O	Date of reading	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

This table contains only the cooling meter data points of a combined heat/cooling meter (Medium = 0Dh). For heat meter data points refer to heat meter for heat meter.

	Cooling	**5**	**$0D_h$ (cooling)**	**(Combined heat/cooling)**					
M	Meter reading	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	
		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
	–	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	
		GJ	10e-9 … 10e-2	0000 cccc		1000 1nnn	0011 1100		
		GJ	10e-1 … 10e+0	0000 cccc		1111 1011	1000 100n	0011 1100	
		GJ	10e+2 … 10e+3	0000 cccc		1111 1011	1000 100n	1111 1101	0011 1100
O	Meter reading	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+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	
	–	kWh	10e-6 … 10e+1	0100 cccc		1000 0nnn	0011 1100		
	–	kWh	10e+2 … 10e+3	0100 cccc		1111 1011	1000 000n	0011 1100	
	–	kWh	10e+5 … 10e+6	0100 cccc		1111 1011	1000 000n	1111 1101	0011 1100
	–	GJ	10e-9 … 10e-2	1100 cccc	0001 0000	0000 1nnn			
	–	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	
	–	GJ	10e-9 … 10e-2	0100 cccc		1000 1nnn	0011 1100		
	–	GJ	10e-1 … 10e+0	0100 cccc		1111 1011	1000 100n	0011 1100	
	–	GJ	10e+2 … 10e+3	0100 cccc		1111 1011	1000 100n	1111 1101	0011 1100
O	Meter reading	5-0:2.0.0*255	Volume (V), accumulated, total, current value						
	–	m^3	10e-6 … 10e+1	0000 cccc		0001 0nnn			
	–	m^3	10e-3 … 10e+4	0000 cccc		1001 0nnn	0111 1101		
O	Meter reading	5-0:2.2.0*255	Volume (V), accumulated, total, set date value						
	–	m^3	10e-6 … 10e+1	0100 cccc		0001 0nnn			
	–	m^3	10e-3 … 10e+4	0100 cccc		1001 0nnn	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	Temperatur	5-0:10.0.0*255	Flow temperature, current value			
	–	℃	10e-3 … 10e+0	0000 cccc		0101 10nn
O	Temperatur	5-0:11.0.0*255	Return temperature, current value			
	–	℃	10e-3 … 10e+0	0000 cccc		0101 11nn
O	Time of device	5-0:0.9.1*255	Current time at time of transmission			
	–	Type F		1000 0100	0001 0000	0110 1101
O	Date of device	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	Time, date of reading	5-0:0.1.2*255	Run time difference between measurement of current value and transmission			
				0000 cccc		0111 01nn
O	Date of reading	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

	Heat	**6**	**04_h, $0C_h$, $0D_h$(heat)**	**(Heat only and combined heat/cooling)**			
M	Meter reading	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 reading	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	Meter reading	6-0:2.0.0*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 reading	6-0:2.2.0*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	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	Temperatur	6-0:10.0.0*255	Flow temperature, current value				
	–	℃	10e-3 … 10e+0	0000 cccc	0101 10nn		
O	Temperatur	6-0:11.0.0*255	Return temperature, current value				
	–	℃	10e-3 … 10e+0	0000 cccc	0101 11nn		

O	Time of device	6-0:0.9.1*255	Current time at time of transmission		
	–	Type F		`0000 0100`	`0110 1101`
O	Date of device	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	Time, date of reading	6-0:0.1.2*255	Run time difference between measurement of current value and transmission		
				`0000 cccc`	`0111 01nn`
O	Date of reading	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 reading	7-0:3.0.0*255	Volume (meter), measuring conditions (V_m), forward, 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 reading	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 reading	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 reading	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 reading	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 reading	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})						
	–	℃	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 device	7-0:0.9.1*255	Current time at time of transmission				
	–	Type F		0000 0100			0110 1101
O	Date of device	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	Time, date of reading	7-0:0.1.2*255	Run time difference between measurement of current value and transmission				
				0000 cccc			0111 01nn
O	Date of reading	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 reading	8-0:1.0.0*255	Volume (*V*), accumulated, total, current value			
	–	m^3	10e-6 … 10e+1	`0000 cccc`	`0001 0nnn`	
	–	m^3	10e-3 … 10e+4	`0000 cccc`	`1001 0nnn`	`0111 1101`
O	Meter reading	8-0:1.2.0*255	Volume (*V*), accumulated, total, set date value			
	–	m^3	10e-6 … 10e+1	`0100 cccc`	`0001 0nnn`	
	–	m^3	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			
	–	m^3/h	10e-6 … 10e+1	`0000 cccc`	`0011 1nnn`	
O	Time of device	8-0:0.9.1*255	Current time at time of transmission			
	–	Type F		`0000 0100`	`0110 1101`	
O	Date of device	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	Time, date of reading	8-0:0.1.2*255	Run time difference between measurement of current value and transmission			
				`0000 cccc`	`0111 01nn`	
O	Date of reading	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 reading	9-0:1.0.0*255	Volume (*V*), accumulated, total, current value			
	–	m^3	10e-6 … 10e+1	0000 cccc	0001 0nnn	
	–	m^3	10e-3 … 10e+4	0000 cccc	1001 0nnn	0111 1101
O	Meter reading	9-0:1.2.0*255	Volume (*V*), accumulated, total, set date value			
	–	m^3	10e-6 … 10e+1	0100 cccc	0001 0nnn	
	–	m^3	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			
	–	m^3/h	10e-6 … 10e+1	0000 cccc	0011 1nnn	
O	Time of device	9-0:0.9.1*255	Current time at time of transmission			
	–	Type F		0000 0100	0110 1101	
O	Date of device	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	Time, date of reading	9-0:0.1.2*255	Run time difference between measurement of current value and transmission			
				0000 cccc	0111 01nn	
O	Date of reading	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 (refer to Table 12).

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 (binary is always unsigned). It is declared in the low nibble of the original DIF (marked with bold) which has to be replaced by length and coding of OBIS code. (Use "binary" if recent value (OBIS F) > 99.)

Example: Max. flow rate of a water meter

A water meter supports a maximum flow rate value e.g. 0,123 m^3/h

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

1Ah	DIF; maximum value; 4 digits BCD
3Bh	VIF; Flow rate with unit 10-3 m^3/h
23h 01h	Value 0123

The relevant OBIS declaration 8-0:2.5.0*255 will be transmitted either binary or with BCD-numbers.

BCD-coding:

The relevant OBIS declaration will be transmitted as 12 digits BCD by

1Eh	DIF; maximum value; 12 digits BCD
BBh	VIF; Flow rate with unit 10-3 m3/h; VIFE follows
3Fh	VIFE "OBIS declaration"
AAh 00h 05h 02h 00h 08h	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 [EN 13757-3]). This corresponds to a recent value of 255.

Binary coding:

Alternative the relevant OBIS declaration will be transmitted e.g. as 48 bit binary by

16h	DIF; maximum value; 48 bit binary
BBh	VIF; flow rate with unit 10^{-3} m3/h; VIFE follows
3Fh	VIFE "OBIS declaration"
FFh 00h 05h 02h 00h 08h	Value; OBIS code 8-0:2.5.0*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 × 1.5 mA + 20 mA (Space) = 29 mA
- Min. Mark voltage under mark/space current (max. 29 mA): 24 V
- Min. Space voltage under mark current (max. 9 mA): 12 V
- Resulting max. idle power: 24 V × 9 mA = 216 mW
- Baud rates: 300 and 2400 Baud
- Collision detect: For bus currents > 30 mA the bus voltage may drop below 24 V. Bus currents > 50 mA shall be signalled to the processor as a heavy collision state. This is required to support all the function of a wildcard-search.
- Galvanic isolation: As required in 4.3.3.9 of [EN 13757-2]
- Symmetry as required in 4.3.3.10 of [EN 13757-2]. DC symmetry requirements may be realized. This may be solved e.g. by a high resistance (2 × 1 MOhm) voltage divider. AC-symmetry may be realized via a (parallel) capacitive divider of e.g. 2 × 1 nF.

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

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

None Header

The None Header may used on wired M-Bus or for none OMS-messages

APL without Header

No message identification by access number, status or encryption possible.

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

CI	Data

Short Header

The Short Header could be applied if the meter application address is identical with the link address of the meter.

APL with Short Header

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

CI	ACC	STS	Conf.Word	AES-Check	Data

TPL with Short Header

- Applied from slave with 8Ah

CI	ACC	STS	Conf.Word

Long Header

If the meter application address differs from the link address of the meter (wM-Bus); the Long Header with support of mandatory secondary address shall be used.

APL with Long Header

- Applied from master with CI = 5Bh; 60h; 64h; 6Ch, 6Dh, 80h
- Applied from slave with CI = 6Fh; 72h; 75h; 7Ch; 7Eh

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

TPL with Long Header

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

CI	Ident. no	Manuf.	Ver.	Med.	ACC	STS	Conf.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)
Conf.Word	Configuration 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 [EN 13757-3] (2004):

Table 17 — Extension list of application errors

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.

5

These application errors are currently defined in [EN 13757-3] (2004) Table 14:

Table 18 — List of application errors based on the existing standard

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 DIFEs
6	More than 10 VIFEs
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 (even if the clock command not applied). The MUC 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 [EN 13757-3]. The TC-Field is used for control timing actions and is defined as:

Table 19 — TC-Field Clock Synchronisation

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)

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 byte = 0)	Command verification (4 byte = 4 × ”2Fh”)

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

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 byte = 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 N (SND-UD).

Annex G1 (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.

Table 20 — Example: Load profile of consumption values for a water meter

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

This load profile should be transmitted as follows:

Table 21 — Coding of the example: Load profile of consumption values for a water meter

Description	DIF/DIFE (Hex)	VIF/VIFE (Hex)	Value (Hex/BCD) (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 G2 (Informative): Transmission of a compact Load Profile

General

The M-Bus compact profiles are used to transport a series of values with a fix space between each value. In addition to the compact profile a base value and a base time is required to declare a start time and the value of the profile. Additional base parameters like the OBIS declaration may be added as well. The base time is chained with the compact profile by using the same Storage number in the DIF/DIFE. The base value and the base parameters are chained with the compact profile by using the same Storage-, Tariff- and Subunit numbers in the DIF/DIFE of the data record. If one of this numbers differs from the compact profile, it has to be assumed that the base value or base parameters are missed.

The base value and base parameter

The data point base value is the eldest value of the data series. It shall always exist unless the increment mode “Absolute value” (00b) is used. In the absence of the base value, the first entry in the profile is used as the first value of the data series instead. The base value and the base parameters may be used with any DIF/DIFE and VIF/VIFE.

Table 22 — Base value record (connected via Storage-, Tariff-, Subunit number and VIF / VIFEx)

DIF/DIFE	VIF/VIFEx	Base value

The base time

The base time shall be encoded with one of the Types F to J (refer to [EN 13757-3] Annex A). It corresponds to the base value, even if it does not exist. Therefore the first entry in the compact profile is always related to the base time added by one space interval.

Table 23 — Base time record (connected via the storage number)

DIF/DIFE	VIF (time/date Type F … J)	Time/date value

Structure of the compact profile

The compact profile record itself starts (like each M-bus data point) with a DIF (DIFE) and a VIF (VIFE) but with an additional (new) orthogonal VIFE signalling a “compact profile”.

The profile record uses a data structure with variable length (DIF = xDh) followed by a length byte with values between 3 and 191 (0BFh). The whole length is accumulated by two control bytes plus N*(element length), where N is the number of elements of the profile. In consequence the length of “2” signals an empty profile.

Table 24 — Profile record (connected via Storage-, Tariff-, Subunit number and VIF/VIFEx)

DIF/DIFE with variable length DIF=xDh	VIF/VIFEx VIFE = 1Eh/1Fh	LVAR # bytes (03h to BFh)	Spacing control byte	Spacing value byte	Oldest Profile Value	…

NOTE: For the binary integers (low nibble of the DIF=1 to 4, 6 or 7) the incremental modes 01b and 10b use unsigned integers (data type C), whereas the increment modes 00b and 11b use signed integers (data type B). Refer to [EN 13757-3] Annex A.

The first byte (Spacing control byte) of this variable length record structure contains the data size of each individual element in the lower four bits (as in the lower nibble of the DIF definitions, but excluding variable length elements). The next higher two bits signal the time spacing units (00b = sec, 01b = min, 10b = hours and 11b = days). The highest two bits signal the increment mode of the profile (00b = absolute value (signed), 01b = positive (unsigned) increments, 10b = negative (unsigned) increments, 11b = signed difference (deviation of last value – next value)). All values of the profile are initially preset with the coding for “illegal”, e.g. -128 for signed byte, 255 for unsigned byte, -32768 for signed word etc (refer to [EN 13757-3] Annex A, type B and C). Invalid values shall also be used in case of an overflow of an incremental value.

Table 25 — Spacing control byte

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}

Table 26 — Structure of Spacing control byte

bit 6 … 7: Increment mode	bit 4 … 5: Spacing unit	bit 0 … 3: Element size
00b = Absolute value	00b = seconds	Profile DIF, low nibble only, but except 0Dh and except 0Fh
01b = Increments	01b = minutes	
10b = Decrements	10b = hours	
11b = Signed difference	11b = days/month	

After the Space control byte follows the Space value byte (single byte) giving the number of the time spacing units between the profile values. It allows between 1 and 250 time units (s, m, h, d) as time spacing. The values 0, 251, 252 and 255 are reserved. To be able to additionally code monthly and half-monthly profile spacing, the value 253 is used for half-monthly spacing and the value 254 is used for monthly spacing. Both are used together with the spacing unit “days/month”.

Table 27 — Spacing value byte

Spacing value	**Spacing unit**	**Meaning**
1 – 250	all	number of days, hours, minutes or seconds between values
251	all	Reserved
252	all	Reserved
253	00b – 10b 11b	reserved; number of half month between values
254	00b – 10b 11b	Reserved number of full month between values
255	all	Reserved

These first two fixed bytes are followed by the oldest value of the profile, the next oldest value etc. until the end of the variable length structure is reached. Note that if each profile value uses a DIF- data format with a length of more than one byte, each individual profile value is in the “least significant byte first” order.

Types of Compact profile

The M-Bus supports two types of compact profiles

- "Compact profile with registers" for the transport of a limited number of values with an assigned register number (e.g. recent value)
- "Compact profile without registers" for the transport of an unlimited number of values as a series with no assignment to a register (e.g. load profile)

The definition of both compact profile types is identical with an exception in the use of the Storage number. The transmission of several profiles (e.g. for two tariffs) in parallel is possible, but it requires a different coding in the DIF/DIFE or the VIF/VIFE e.g. by the use of different Tariff numbers. As long as the Storage numbers are identical, all compact profiles are related to the same base time.

Compact profile with registers (orthogonal VIFE = 1Eh)

This compact profile has to be selected if the assignment of a historical value to a cumulation register is required.

The first requested register number is coded by the storage number which is used for the base time, the base value and the compact profile. The first value inside the compact profile is related to the second requested register number, the second value to the third register and so on. To support up to 125 registers, a fix coding with a DIF and two DIFEs shall always be used.

A data series may also contain non periodic entries e.g. in the case of a changed device status. Such a case can be transmitted by chaining several profiles (see in example).

Example: absolute profile of monthly consumption values (Tariff 1) of an electricity meter

Table 28 — Example of compact profile with registers: Plain data

Event	OBIS code	Date/Time	Value
periodic value	1.8.1*32	01.01.2010 00:00	150 kWh
periodic value	1.8.1*33	01.02.2010 00:00	100 kWh
periodic value	1.8.1*34	01.03.2010 00:00	130 kWh
non periodic value	1.8.1*35	25.03.2010 13:12	90 kWh
periodic value	1.8.1*36	01.04.2010 00:00	50 kWh
periodic value	1.8.1*37	01.05.2010 00:00	160 kWh

Table 29 — Example of compact profile with registers: M-Bus data records

Data point type	Stor.	Tariff	M-Bus data record
Base time	#32	T0	86h 80h 01h 6Dh 00h 00h A0h 41h 11h 35h
Base value	#32	T1	84h 90h 01h 03h F0h 49h 02h 00h
Profile 1 (2 values: #33; #34)	#32	T1	8Dh 90h 01h 83h 1Eh 0Ah 04h FEh A0h 86h 01h 00h D0h FBh 01h 00h
Base time	#35	T0	C6h 81h 01h 6Dh 0Bh 0Ch 8Dh 59h 13h 0Ch
Base value	#35	T1	C4h 91h 01h 03h 90h 5Fh 01h 00h
Base time	#36	T0	86h 82h 01h 6Dh 00h 00h 80h 41h 14h 0Dh
Base value	#36	T1	84h 92h 01h 03h 50h C3h 00h 00h
Profile 2 (1 value: #37)	#36	T1	8Dh 92h 00h 83h 1Eh 06h 04h FEh 00h 71h 02h 00h

Compact profile without registers (orthogonal VIFE = 1Fh)

The compact profiles without registers shall start with the Storage number #8. They may use a flexible number of DIFs and DIFEs. Chained compact files without registers use (unlike the compact files with registers) the next higher Storage number. The use of the Storage number #0 is not permitted for compact files without registers.

Example: incremental load profile; 3 hourly volume values after midnight coded with BCD.

Table 30 — Example of compact profile without registers: Plain data

Base value	01.01.2010 00:00	12300.0 m^3
Oldest profile value	01.01.2010 01:00	12300.3 m^3
Second oldest value	01.01.2010 02:00	12300.5 m^3
Third oldest value	01.01.2010 03:00	12301.6 m^3

Table 31 — Example of compact profile without registers: M-Bus data records

Data point type	Stor.	Tariff	M-Bus data record
Base time	#8	T0	84h 04h 6Dh 00h 20h 41h 11h
Base value	#8	T0	8Bh 04h 15h 00h 30h 12h
Profile	#8	T0	8Dh 04h 95h 1Fh 05h 69h 01h 03h 02h 11h

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

Glossary

Table 32 — Glossary of the Gas meter consumption data

V_m	The volume at measurement conditions
V_{tc}	Temperature converted volume
V_b	The volume at base conditions
Measurement conditions	Conditions of the gas whose volume is measured at the point of measurement (e.g. the temperature and the pressure of the gas) EN 12405:2002 3.1.2
Base conditions	Fixed conditions used to express the volume of gas independently of the measurement conditions EN 12405:2002 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

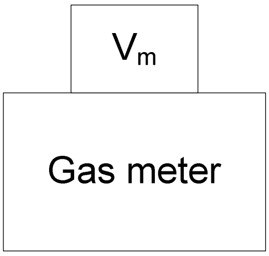
The conversion from the volume at measurement conditions (V_m) to the volume at base conditions (V_b) can be done by the gas meter, by a conversion device and/or by the billing system. Gas meter with build in temperature conversion device convert V_m to V_{tc}.

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

Volume at Measurement Conditions

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



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

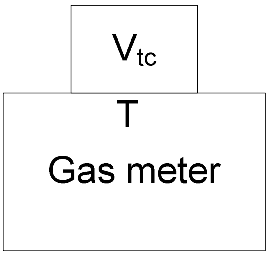
Suitable OBIS and M-Bus codes can be found in Annex A.

Temperature Converted Volume V_{tc}

An individual meter based volume conversion to V_{tc} (in contrast to the “global” billing centre based conversion) can be achieved either mechanically or electronically. It can be implemented either internally in the meter or by some external conversion device which then transmits converted values to the billing centre. Note that such a temperature conversion is based on a base temperature, which must be known to the billing centre. The default value for such a temperature at base conditions is 15 ℃ according t o 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 centre to its “billing temperature at base conditions” if this is different either from the default temperature of 15 ℃ 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

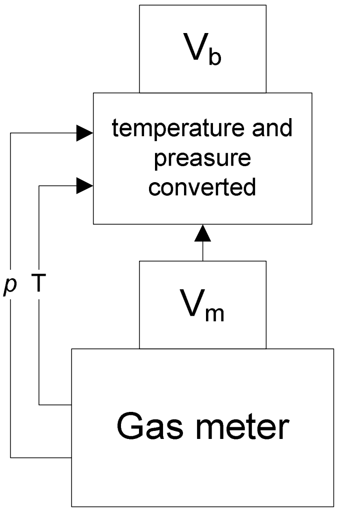
In addition to a volume conversion just regarding temperature an individual meter might convert its measured volume to base conditions regarding temperature and pressure. To comply with standard conditions, which are usually stated by national regulations and to allow the creation of gas bills that can 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 centre. The default value for such a pressure at base conditions is 1013.25 mbar. If a meter uses a different value for pressure at base conditions such pressure at base conditions information shall be added to each volume data telegram.

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



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

OBIS / COSEM Application of Physical Units for Gas

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

Table 33 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.

Table 33 — Enumerated values for physical units

unit ::= enum	**Unit**	**Quantity**	**Unit name**	**SI definition (comment)**
(9)	°C	temperature (T)	Degree Celsius	K - 273.15
(13)	m^3	volume (V) r_V , meter constant or pulse value (volume)	cubic meter	m^3
(14)	m^3	Converted volume	cubic meter	m^3
(19)	l	Volume	Litre	10^{-3} m^3
(23)	Pa	pressure (p)	Pascal	N/m^2
(24)	bar	pressure (p)	Bar	10^5 N/m^2
(52)	K	temperature (T)	Kelvin	

Some examples are shown in Table 34 below.

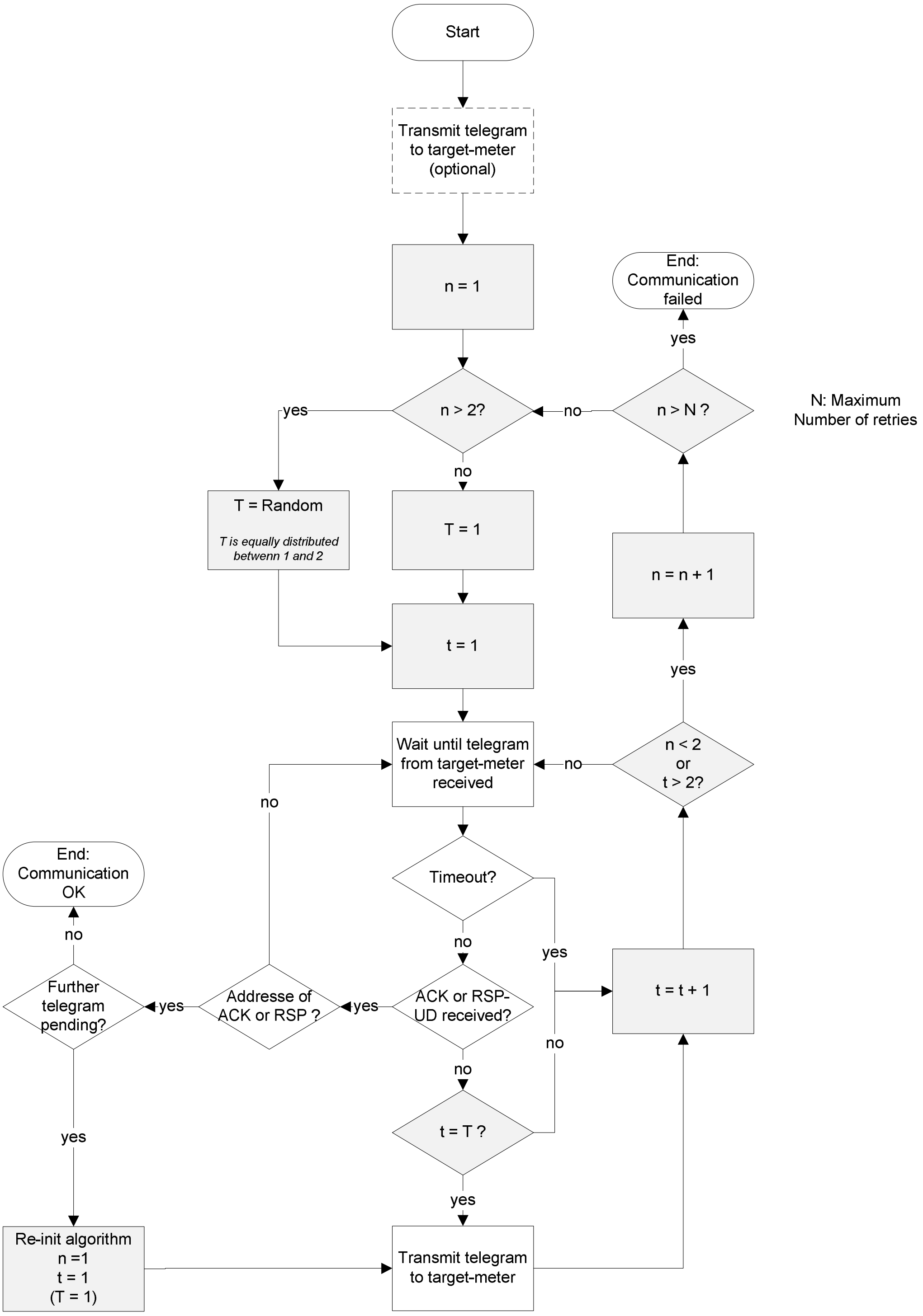
Table 34 — Examples for scaler-unit

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

Annex I (Normative): Collision Avoiding Mechanism of the 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


Start
Transmit telegram to target-meter (optional)
n = 1
n > 2?
yes
no
T = Random
T is equally distributed betwenn 1 and 2
T = 1
t = 1
End: Communication failed
yes
n > N ?
no
N: Maximum Number of retries
n = n + 1
yes
n < 2 or t > 2?
no
Wait until telegram from target-meter received
no
Timeout?
yes
no
t = t + 1
End: Communication OK
no
Further telegram pending?
yes
Addresse of ACK or RSP ?
yes
ACK or RSP-UD received?
no
no
t = T ?
yes
yes
Re-init algorithm n =1 t = 1 (T = 1)
Transmit telegram to target-meter

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 [5].

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.

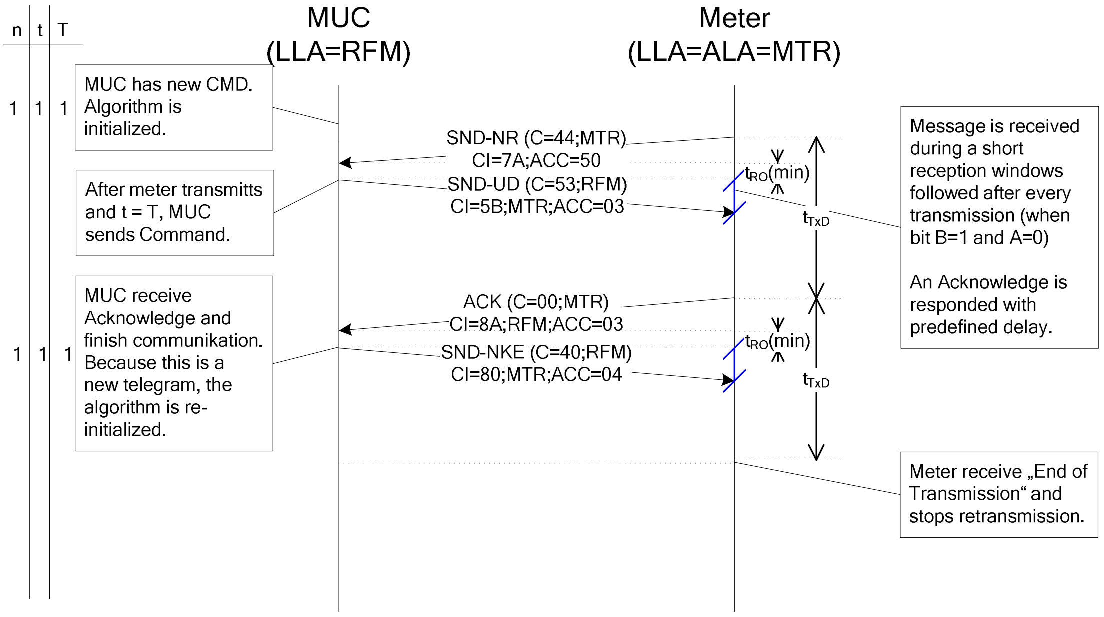
Example: Access of one MUC without Collision

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 behaviour versus time together with the three variables of the algorithm.

[5] 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

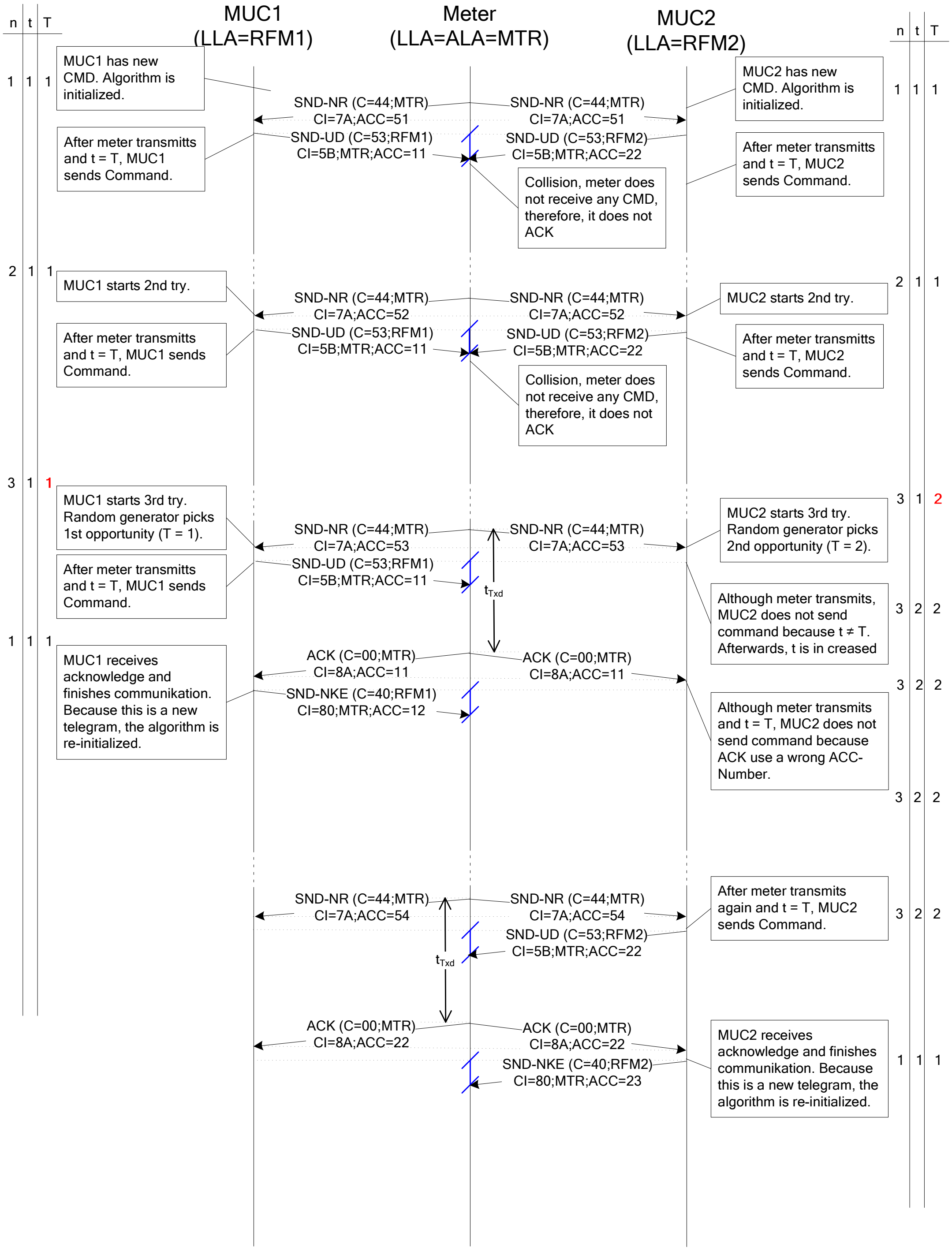

n
t
T
MUC
(LLA=RFM)
Meter
(LLA=ALA=MTR)
1
1
1
MUC has new CMD. Algorithm is initialized.
After meter transmitts and t = T, MUC sends Command.
MUC receive Acknowledge and finish communikation. Because this is a new telegram, the algorithm is re-initialized.
1
1
1
SND-NR (C=44;MTR)
CI=7A;ACC=50
SND-UD (C=53;RFM)
CI=5B;MTR;ACC=03
ACK (C=00;MTR)
CI=8A;RFM;ACC=03
SND-NKE (C=40;RFM)
CI=80;MTR;ACC=04
tRO(min)
tTxD
tRO(min)
tTxD
Message is received during a short reception windows followed after every transmission (when bit B=1 and A=0)
An Acknowledge is responded with predefined delay.
Meter receive „End of Transmission“ and stops retransmission.

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


n t T
MUC1 (LLA=RFM1)
Meter (LLA=ALA=MTR)
MUC2 (LLA=RFM2)
n t T
1 1 1
MUC1 has new CMD. Algorithm is initialized.
MUC2 has new CMD. Algorithm is initialized.
1 1 1
SND-NR (C=44;MTR) CI=7A;ACC=51
SND-NR (C=44;MTR) CI=7A;ACC=51
After meter transmitts and t = T, MUC1 sends Command.
SND-UD (C=53;RFM1) CI=5B;MTR;ACC=11
SND-UD (C=53;RFM2) CI=5B;MTR;ACC=22
After meter transmitts and t = T, MUC2 sends Command.
Collision, meter does not receive any CMD, therefore, it does not ACK
2 1 1
MUC1 starts 2nd try.
SND-NR (C=44;MTR) CI=7A;ACC=52
SND-NR (C=44;MTR) CI=7A;ACC=52
MUC2 starts 2nd try.
2 1 1
After meter transmitts and t = T, MUC1 sends Command.
SND-UD (C=53;RFM1) CI=5B;MTR;ACC=11
SND-UD (C=53;RFM2) CI=5B;MTR;ACC=22
After meter transmitts and t = T, MUC2 sends Command.
Collision, meter does not receive any CMD, therefore, it does not ACK
3 1 1
MUC1 starts 3rd try. Random generator picks 1st opportunity (T = 1).
SND-NR (C=44;MTR) CI=7A;ACC=53
SND-NR (C=44;MTR) CI=7A;ACC=53
MUC2 starts 3rd try. Random generator picks 2nd opportunity (T = 2).
3 1 2
After meter transmitts and t = T, MUC1 sends Command.
SND-UD (C=53;RFM1) CI=5B;MTR;ACC=11
t_Txd
Although meter transmits, MUC2 does not send command because t ≠ T. Afterwards, t is in creased
3 2 2
1 1 1
MUC1 receives acknowledge and finishes communikation. Because this is a new telegram, the algorithm is re-initialized.
ACK (C=00;MTR) CI=8A;ACC=11
ACK (C=00;MTR) CI=8A;ACC=11
SND-NKE (C=40;RFM1) CI=80;MTR;ACC=12
3 2 2
Although meter transmits and t = T, MUC2 does not send command because ACK use a wrong ACC-Number.
3 2 2
SND-NR (C=44;MTR) CI=7A;ACC=54
SND-NR (C=44;MTR) CI=7A;ACC=54
After meter transmits again and t = T, MUC2 sends Command.
3 2 2
SND-UD (C=53;RFM2) CI=5B;MTR;ACC=22
t_Txd
ACK (C=00;MTR) CI=8A;ACC=22
ACK (C=00;MTR) CI=8A;ACC=22
SND-NKE (C=40;RFM2) CI=80;MTR;ACC=23
MUC2 receives acknowledge and finishes communikation. Because this is a new telegram, the algorithm is re-initialized.
1 1 1

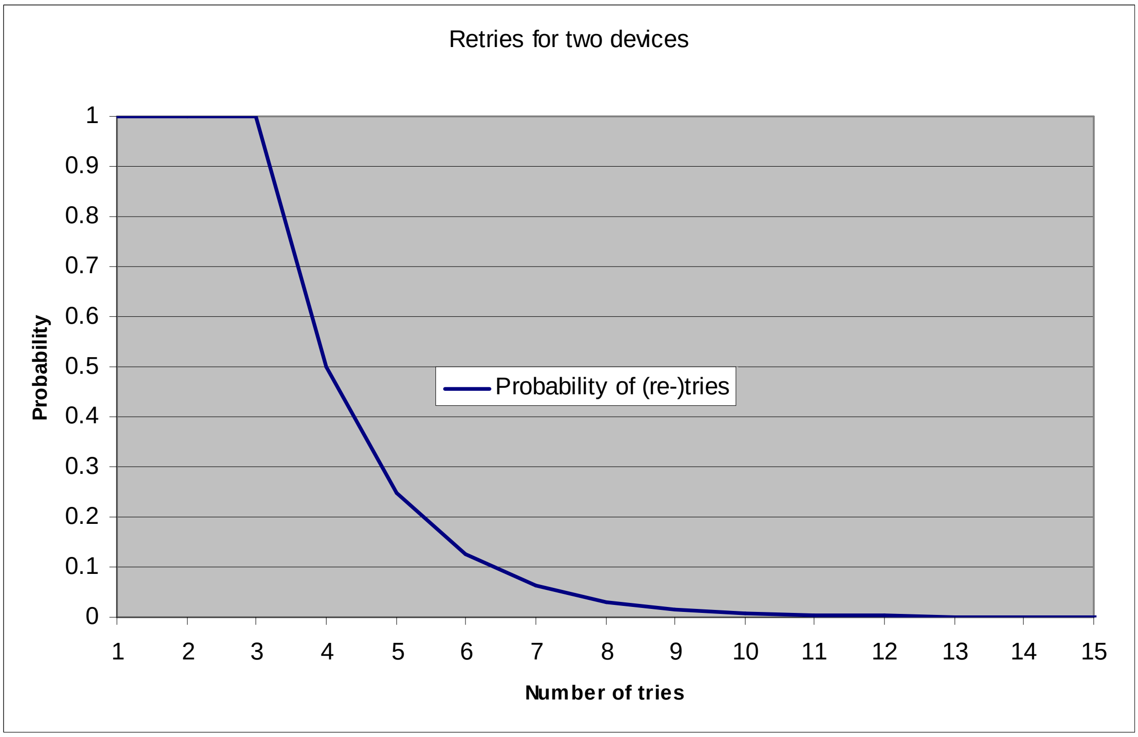
After the collision of the MUCs' first transmission, both start a 3rd try with MUC1 choosing the 1st and MUC2 the 2nd opportunity. As a result, MUC1 transmits the command after the next received telegram, whereas MUC2 waits for the next possibility. Because the following transmissions of the meter are 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 nth try with n larger than 2 is $0.5^2 \times 2 = 0.5$.

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

With the number of tries, the probability decreases that further tries are necessary. For example, the probability to have at least 3 tries is 1 and is the consequence of the 100% collision probability for the 1st and 2nd try. The probability to have at least 4 tries is 1 × 1 × 0.5 and therefore the result of having a collision in the 1st, 2nd and 3rd try. In general, the probability to have the necessity for at least n tries is $1 \times 0.5^{n-2}$ (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**	**Configuration Word**	
				Meter Link-Addr.					*Meter Appl.-Addr.*				*MTR-ACC*	*MTR-ST*	*Conf.word*	*Data*
SND-NR	xx	44	B3 3D	44 33 22 11	55	37	CRC	72	55 66 77 88	B3 3D	44	07	B1	00	20 A5	{2F 2F DIF} CRC {VIF …}CRC
				Meter Link-Addr.					*Meter APL-Addr.*				*MTR-ACC*	*MTR-ST*	*Conf.word*	*No data*
ACC-NR	16	47	B3 3D	44 33 22 11	55	37	CRC	72	55 66 77 88	B3 3D	44	07	B2	00	00 A0	CRC
				MUC-Addr.					*Meter Appl.-Addr.*				*MUC-ACC*	*MUC-ST*	*Conf.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*	*Conf.word*	*Data*
RSP-UD	xx	08	B3 3D	44 33 22 11	55	37	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*	*Conf.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*	*Conf.word*	*no data*
ACK	16	00	B3 3D	44 33 22 11	55	37	CRC	8B	55 66 77 88	B3 3D	44	07	A1	00	00 80	CRC
				MUC-Addr.					*Meter Appl.-Addr.*				*MUC-ACC*	*MUC-ST*	*Conf.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 APL-Addr.*			*MTR-ACC*	*MTR-ST*	*Conf.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*	*Conf.word*	*No data*
CNF-IR	16	06	A3 36	78 56 34 12	9A	31	CRC	80	66 55 44 33	B3 3D	77	03	C2	17	00 C0	CRC

				Meter Link-Addr.						*Meter APL-Addr.*			*MTR-ACC*	*MTR-ST*	*Conf.word*	*No data*
ACC-DMD	0E	48	B3 3D	66 55 44 33	77	03	CRC	8A					C3	00	00 80	CRC
				MUC-Addr.						*Meter Appl.-Addr.*			*MTR-ACC*	*MUC-ST*	*Conf.word*	*No data*
ACK	16	00	A3 36	78 56 34 12	9A	31	CRC	80	66 55 44 33	B3 3D	77	03	C3	00	00 C0	CRC

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

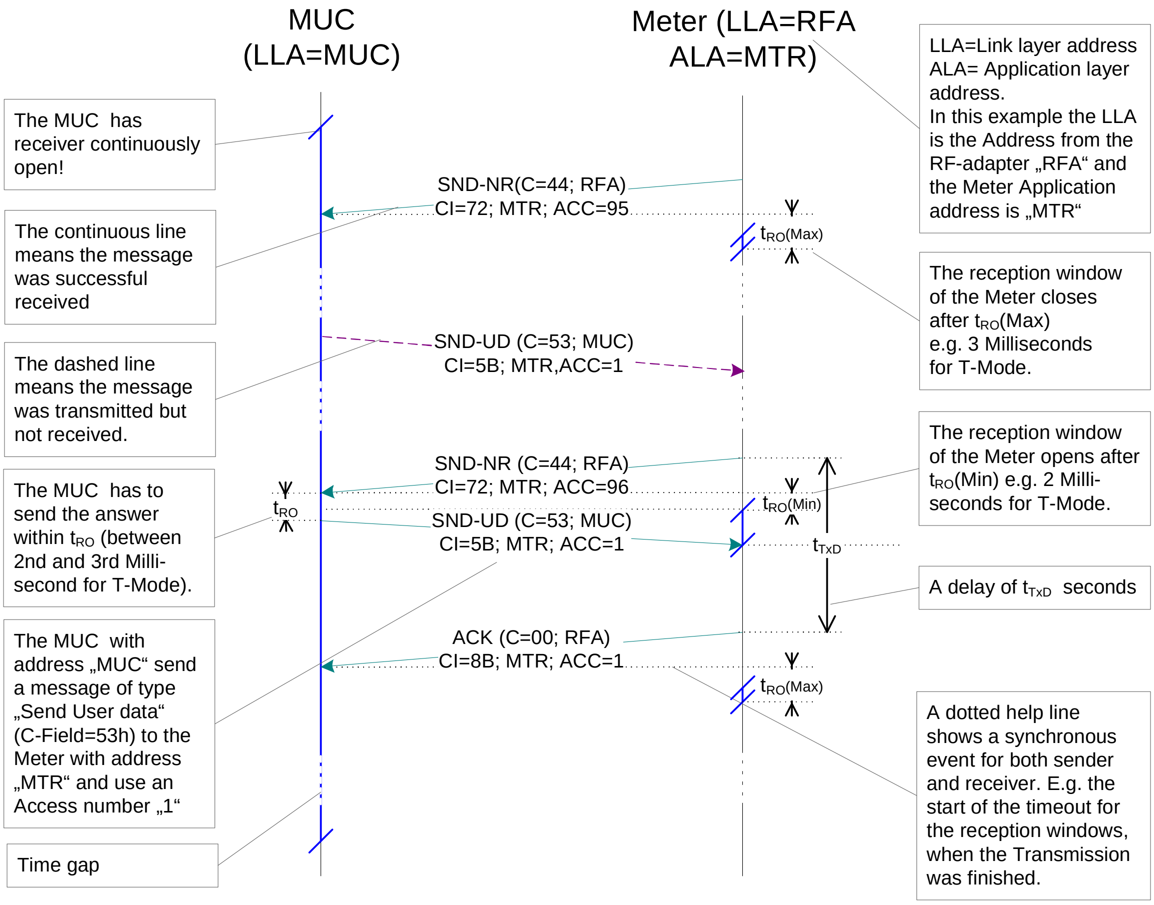
Manuf	15795d	3DB3h	"OMS"
Ident	11223344d	11 22 33 44h	BCD-Coding!
Version	85d	55h	Binäry
Medium	55d	37h	Radio converter

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



The MUC has receiver continuously open!

The continuous line means the message was successful received

The dashed line means the message was transmitted but not received.

The MUC has to send the answer within t_{RO} (between 2nd and 3rd Milli-second for T-Mode).

The MUC with address „MUC“ send a message of type „Send User data“ (C-Field=53h) to the Meter with address „MTR“ and use an Access number „1“

Time gap

LLA=Link layer address
ALA= Application layer address.
In this example the LLA is the Address from the RF-adapter „RFA“ and the Meter Application address is „MTR“

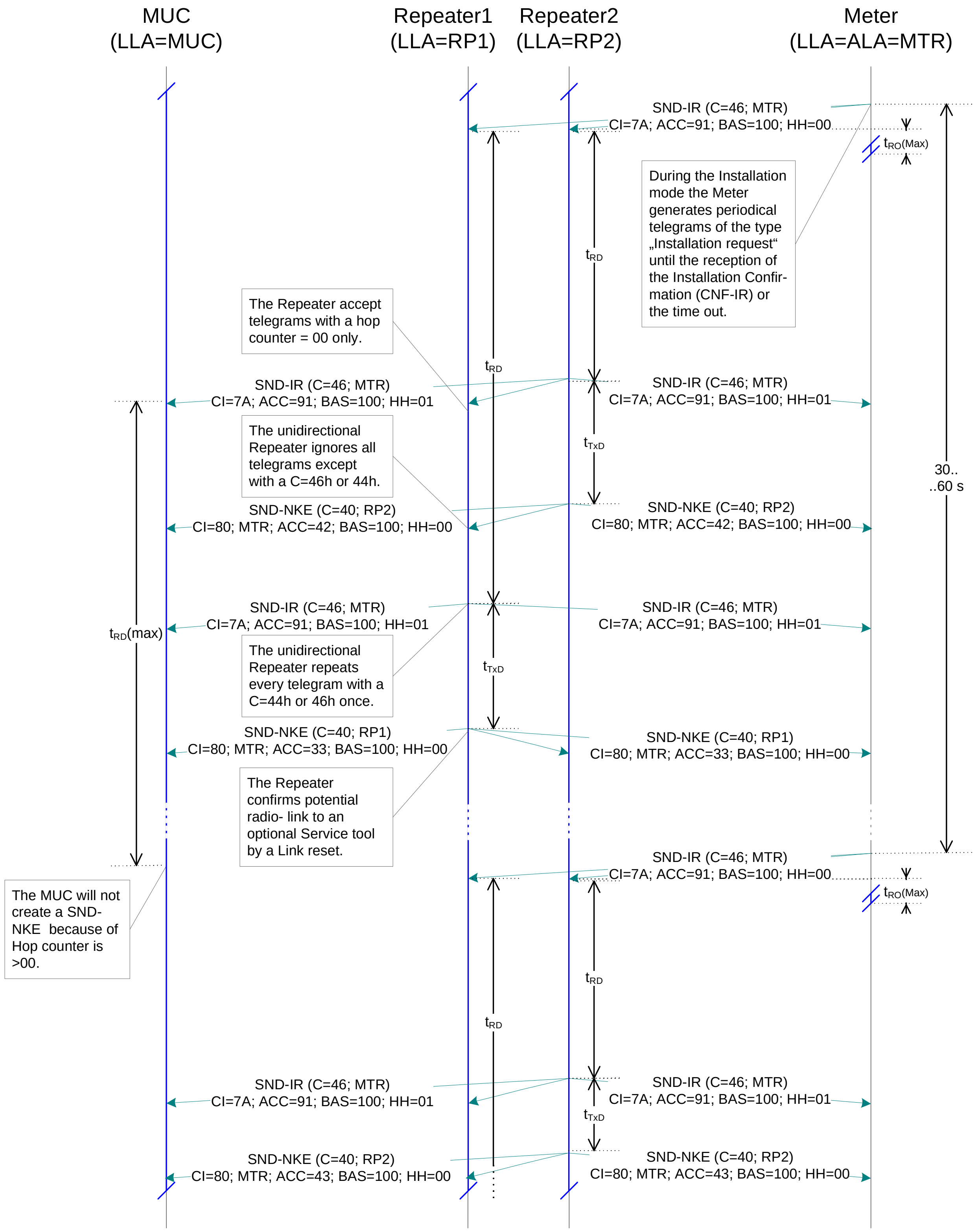
The reception window of the Meter closes after t_{RO}(Max) e.g. 3 Milliseconds for T-Mode.

The reception window of the Meter opens after t_{RO}(Min) e.g. 2 Milli-seconds for T-Mode.

A delay of t_{TxD} seconds

A dotted help line shows a synchronous event for both sender and receiver. E.g. the start of the timeout for the reception windows, when the Transmission was finished.

Installation Procedure with unidirectional Repeaters


MUC
(LLA=MUC)
Repeater1
(LLA=RP1)
Repeater2
(LLA=RP2)
Meter
(LLA=ALA=MTR)
SND-IR (C=46; MTR)
CI=7A; ACC=91; BAS=100; HH=00
tRO(Max)
tRD
tRD
SND-IR (C=46; MTR)
CI=7A; ACC=91; BAS=100; HH=01
SND-IR (C=46; MTR)
CI=7A; ACC=91; BAS=100; HH=01
tTxD
30..
..60 s
SND-NKE (C=40; RP2)
CI=80; MTR; ACC=42; BAS=100; HH=00
SND-NKE (C=40; RP2)
CI=80; MTR; ACC=42; BAS=100; HH=00
SND-IR (C=46; MTR)
CI=7A; ACC=91; BAS=100; HH=01
SND-IR (C=46; MTR)
CI=7A; ACC=91; BAS=100; HH=01
tRD(max)
tTxD
SND-NKE (C=40; RP1)
CI=80; MTR; ACC=33; BAS=100; HH=00
SND-NKE (C=40; RP1)
CI=80; MTR; ACC=33; BAS=100; HH=00
SND-IR (C=46; MTR)
CI=7A; ACC=91; BAS=100; HH=00
tRO(Max)
tRD
tRD
SND-IR (C=46; MTR)
CI=7A; ACC=91; BAS=100; HH=01
SND-IR (C=46; MTR)
CI=7A; ACC=91; BAS=100; HH=01
tTxD
SND-NKE (C=40; RP2)
CI=80; MTR; ACC=43; BAS=100; HH=00
SND-NKE (C=40; RP2)
CI=80; MTR; ACC=43; BAS=100; HH=00

During the Installation mode the Meter generates periodical telegrams of the type „Installation request“ until the reception of the Installation Confirmation (CNF-IR) or the time out.

The Repeater accept telegrams with a hop counter = 00 only.

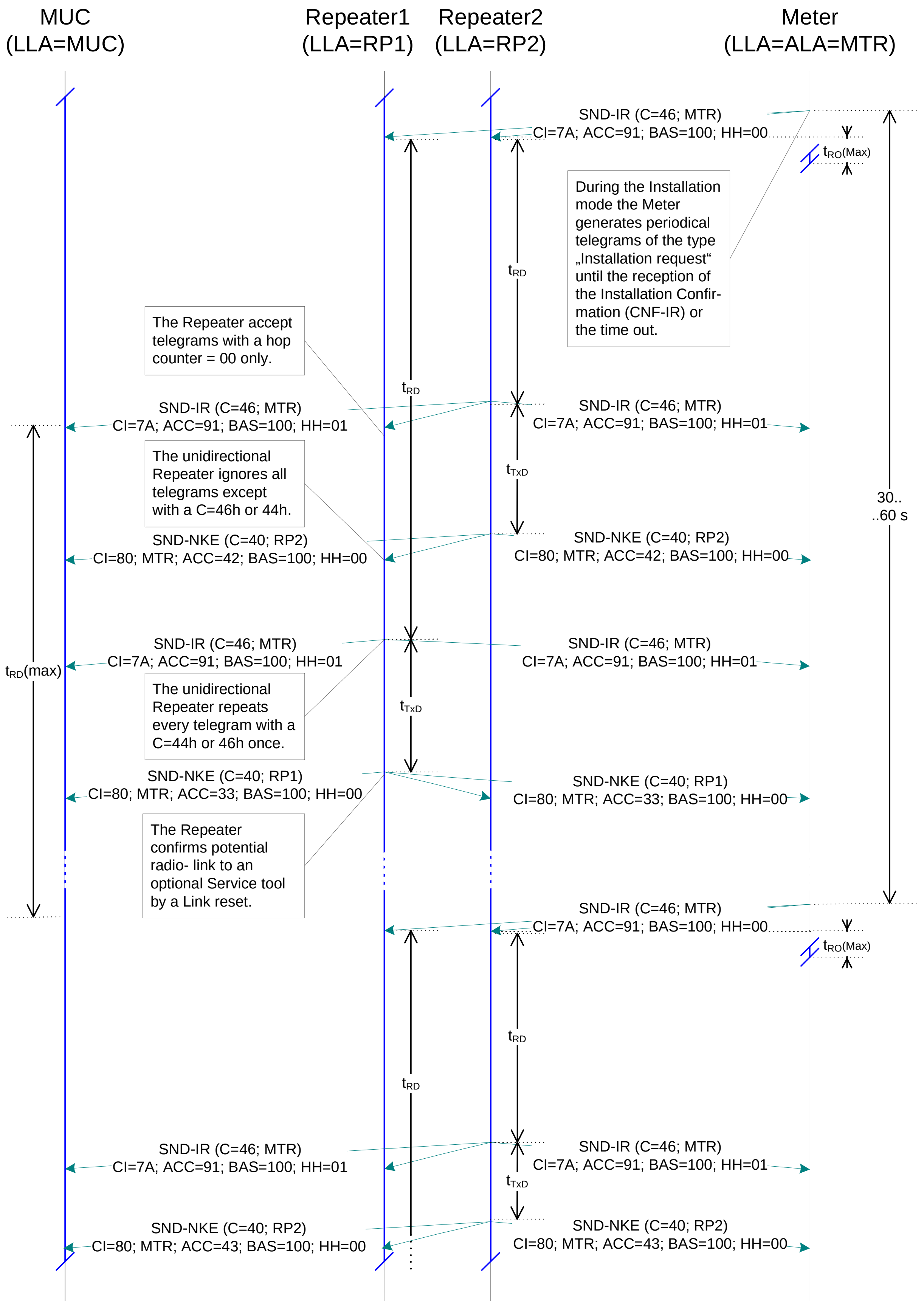
The unidirectional Repeater ignores all telegrams except with a C=46h or 44h.

The unidirectional Repeater repeats every telegram with a C=44h or 46h once.

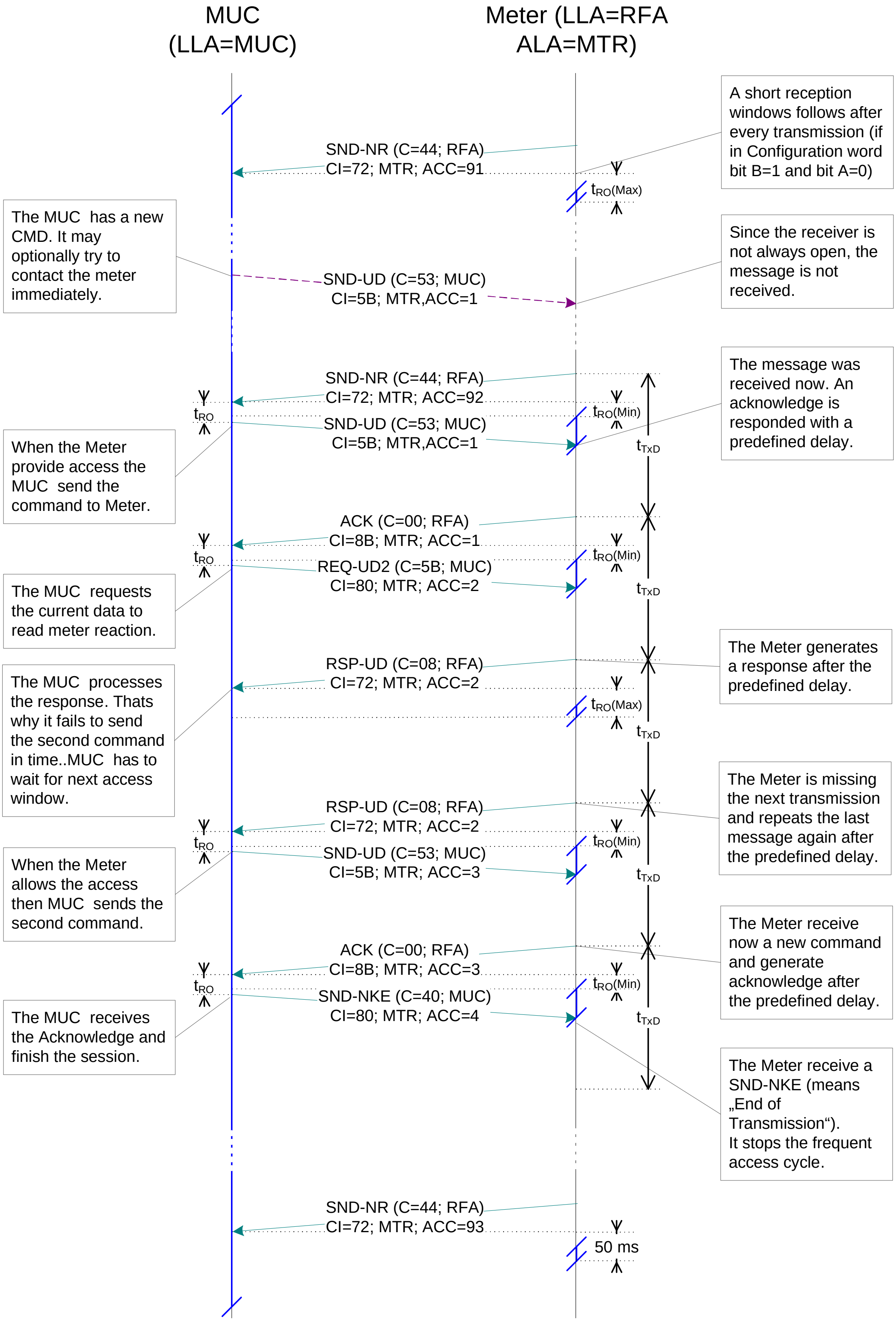
The Repeater confirms potential radio- link to an optional Service tool by a Link reset.

The MUC will not create a SND-NKE because of Hop counter is >00.

Installation Procedure with unidirectional Repeaters


MUC
(LLA=MUC)
Repeater1
(LLA=RP1)
Repeater2
(LLA=RP2)
Meter
(LLA=ALA=MTR)
SND-IR (C=46; MTR)
CI=7A; ACC=91; BAS=100; HH=00
tRO(Max)
30..
..60 s
During the Installation mode the Meter generates periodical telegrams of the type „Installation request" until the reception of the Installation Confir-mation (CNF-IR) or the time out.
tRD
The Repeater accept telegrams with a hop counter = 00 only.
tRD
SND-IR (C=46; MTR)
CI=7A; ACC=91; BAS=100; HH=01
SND-IR (C=46; MTR)
CI=7A; ACC=91; BAS=100; HH=01
The unidirectional Repeater ignores all telegrams except with a C=46h or 44h.
tTxD
SND-NKE (C=40; RP2)
CI=80; MTR; ACC=42; BAS=100; HH=00
SND-NKE (C=40; RP2)
CI=80; MTR; ACC=42; BAS=100; HH=00
SND-IR (C=46; MTR)
CI=7A; ACC=91; BAS=100; HH=01
SND-IR (C=46; MTR)
CI=7A; ACC=91; BAS=100; HH=01
tRD(max)
The unidirectional Repeater repeats every telegram with a C=44h or 46h once.
tTxD
SND-NKE (C=40; RP1)
CI=80; MTR; ACC=33; BAS=100; HH=00
SND-NKE (C=40; RP1)
CI=80; MTR; ACC=33; BAS=100; HH=00
The Repeater confirms potential radio- link to an optional Service tool by a Link reset.
SND-IR (C=46; MTR)
CI=7A; ACC=91; BAS=100; HH=00
tRO(Max)
tRD
tRD
SND-IR (C=46; MTR)
CI=7A; ACC=91; BAS=100; HH=01
SND-IR (C=46; MTR)
CI=7A; ACC=91; BAS=100; HH=01
tTxD
SND-NKE (C=40; RP2)
CI=80; MTR; ACC=43; BAS=100; HH=00
SND-NKE (C=40; RP2)
CI=80; MTR; ACC=43; BAS=100; HH=00

RF-Connection with Long Address



A short reception windows follows after every transmission (if in Configuration word bit B=1 and bit A=0)

The MUC has a new CMD. It may optionally try to contact the meter immediately.

Since the receiver is not always open, the message is not received.

The message was received now. An acknowledge is responded with a predefined delay.

When the Meter provide access the MUC send the command to Meter.

The MUC requests the current data to read meter reaction.

The Meter generates a response after the predefined delay.

The MUC processes the response. Thats why it fails to send the second command in time..MUC has to wait for next access window.

The Meter is missing the next transmission and repeats the last message again after the predefined delay.

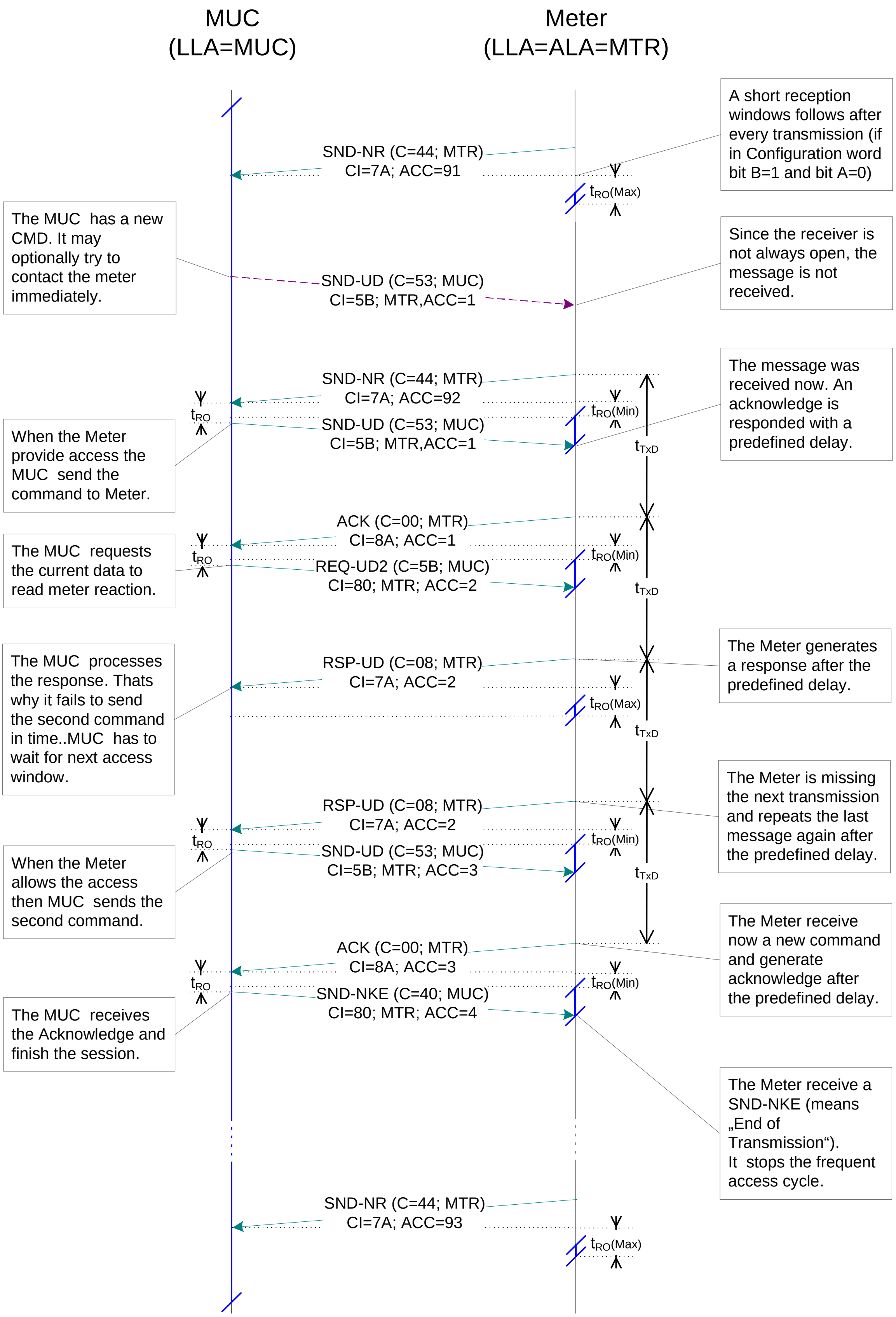
When the Meter allows the access then MUC sends the second command.

The Meter receive now a new command and generate acknowledge after the predefined delay.

The MUC receives the Acknowledge and finish the session.

The Meter receive a SND-NKE (means „End of Transmission“).
It stops the frequent access cycle.

RF-Connection with Short Address



A short reception windows follows after every transmission (if in Configuration word bit B=1 and bit A=0)

The MUC has a new CMD. It may optionally try to contact the meter immediately.

Since the receiver is not always open, the message is not received.

The message was received now. An acknowledge is responded with a predefined delay.

When the Meter provide access the MUC send the command to Meter.

The MUC requests the current data to read meter reaction.

The Meter generates a response after the predefined delay.

The MUC processes the response. Thats why it fails to send the second command in time..MUC has to wait for next access window.

The Meter is missing the next transmission and repeats the last message again after the predefined delay.

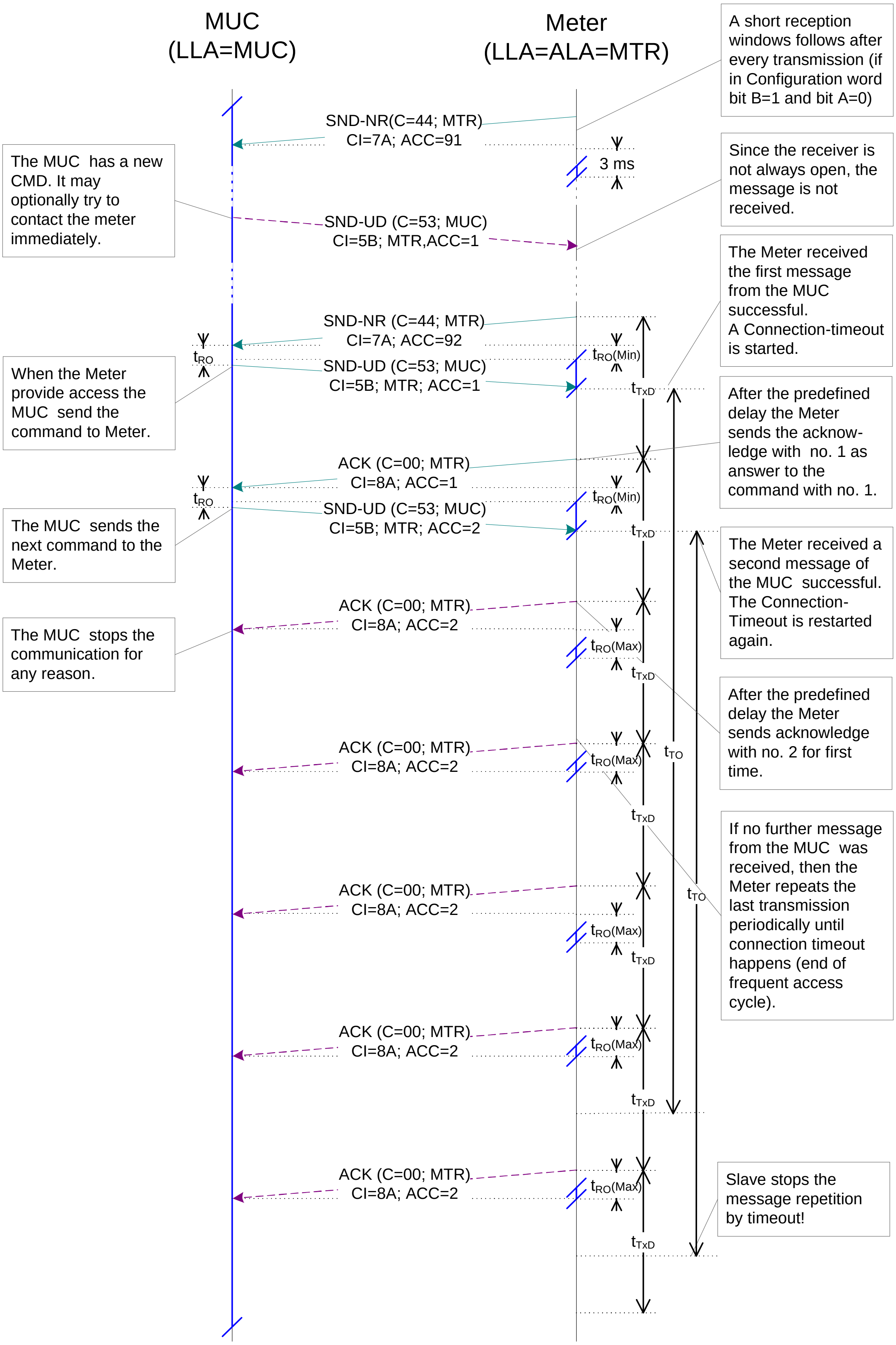
When the Meter allows the access then MUC sends the second command.

The Meter receive now a new command and generate acknowledge after the predefined delay.

The MUC receives the Acknowledge and finish the session.

The Meter receive a SND-NKE (means „End of Transmission“).
It stops the frequent access cycle.

Connection timeout of the Frequent Access Cycle



A short reception windows follows after every transmission (if in Configuration word bit B=1 and bit A=0)

The MUC has a new CMD. It may optionally try to contact the meter immediately.

Since the receiver is not always open, the message is not received.

The Meter received the first message from the MUC successful. A Connection-timeout is started.

When the Meter provide access the MUC send the command to Meter.

After the predefined delay the Meter sends the acknowledge with no. 1 as answer to the command with no. 1.

The MUC sends the next command to the Meter.

The Meter received a second message of the MUC successful. The Connection-Timeout is restarted again.

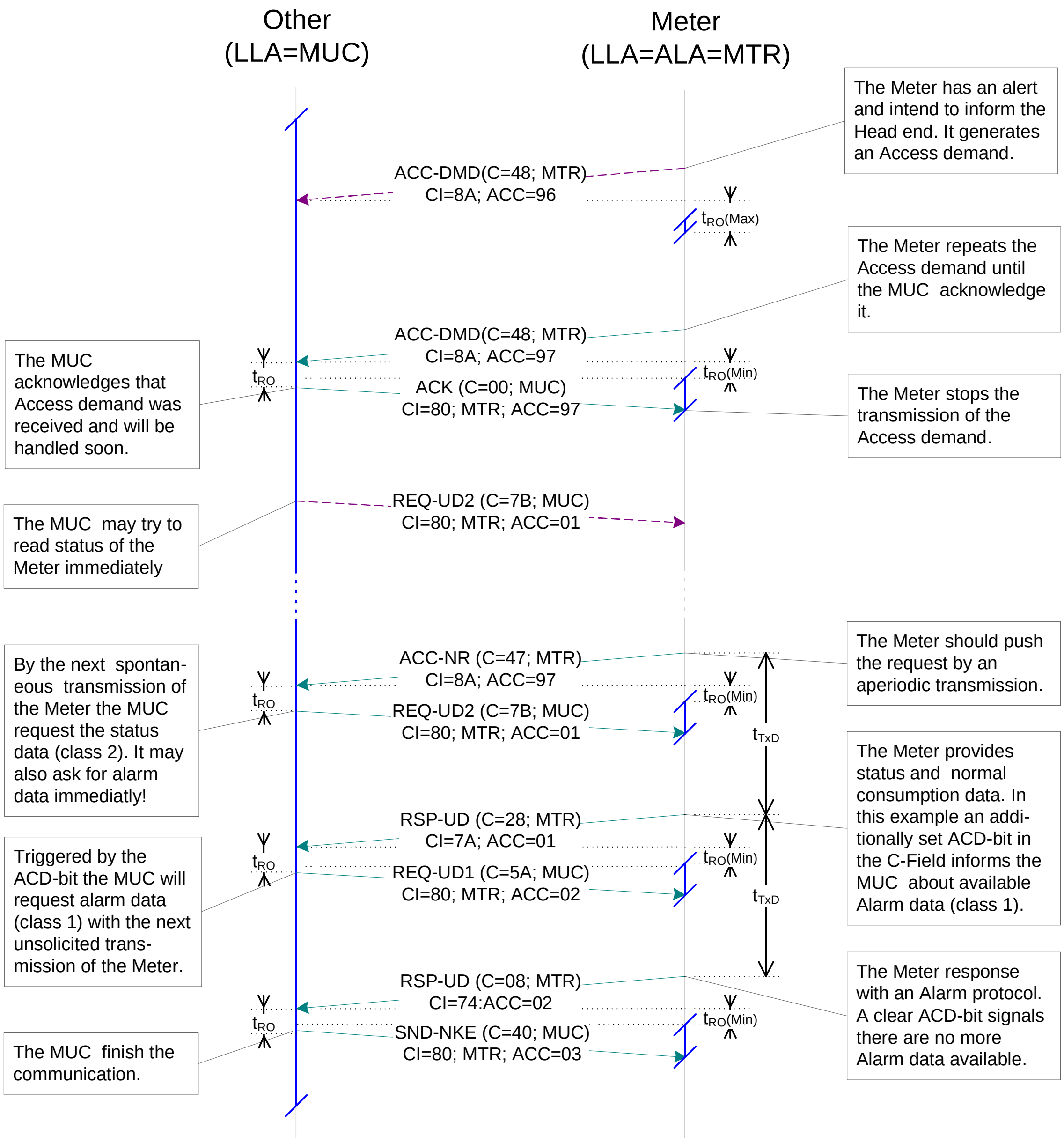
The MUC stops the communication for any reason.

After the predefined delay the Meter sends acknowledge with no. 2 for first time.

If no further message from the MUC was received, then the Meter repeats the last transmission periodically until connection timeout happens (end of frequent access cycle).

Slave stops the message repetition by timeout!

Access Demand from Meter



The Meter has an alert and intend to inform the Head end. It generates an Access demand.

The Meter repeats the Access demand until the MUC acknowledge it.

The MUC acknowledges that Access demand was received and will be handled soon.

The Meter stops the transmission of the Access demand.

The MUC may try to read status of the Meter immediately

The Meter should push the request by an aperiodic transmission.

By the next spontaneous transmission of the Meter the MUC request the status data (class 2). It may also ask for alarm data immediatly!

The Meter provides status and normal consumption data. In this example an additionally set ACD-bit in the C-Field informs the MUC about available Alarm data (class 1).

Triggered by the ACD-bit the MUC will request alarm data (class 1) with the next unsolicited transmission of the Meter.

The Meter response with an Alarm protocol. A clear ACD-bit signals there are no more Alarm data available.

The MUC finish the communication.

Annex M (Informative): Example for a prediction of the next synchronous transmission

To synchronize with the synchronous transmissions of a meter, it is required to receive at least two synchronous frames. To do so with a reasonable failure rate, a continuous reception period of six intervals is recommended. Since the maximum interval is restricted e.g. in Mode T to 15 minutes, 90 minutes of continuous reception are adequate.

Example:

Two synchronous frames with the access number values 110 and 112 have been received at a time distance of 1661.563 s. From the access number values can be seen that one frame has been missed. Thus, the interval between the two frames is:

$1661.563\text{ s} = T_{110} + T_{111}$
$= (1 + (|110 - 128| - 64) / 2048) \times T_{nom} + (1 + (|111 - 128| - 64) / 2048) \times T_{nom}.$
$= (1 + (-46 / 2048) + 1 + (-47 / 2048)) \times T_{nom}$

Now the nominal interval can be determined:

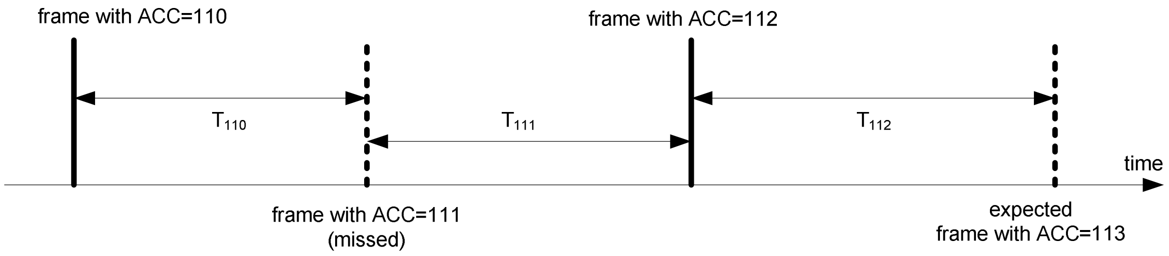
$T_{nom} = 1661.563\text{ s} \times 2048 / (2048 - 46 + 2048 - 47) = 850.083\text{ s}$

The integer factor is N = 425.

With the nominal interval the expected interval to the next synchronous transmission T_{112} can be determined:

$T_{112} = (1 + (|112 - 128| - 64) / 2048) \times 850.083\text{ s} = 830.159\text{ s}$

The nominal interval for that meter can be recalculated after every reception of a new synchronous frame of that meter to compensate temperature drift.



Annex N (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, temperature converted	28504,27 m³
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	Config.word	NNNNCCHHb (2 encr. blocks)	00h	20h		
17	Config.word	BAS0MMMMb (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		
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)

		OMS M-Bus frame	Gas meter example	
Byte No	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	Config.word	no Encryption	00h	
19	Config.word	no Encryption	00h	
20	DR1	DIF (8 digit BCD)	0Ch	
21	DR1	VIF (Volume 0,01 m^3)	14h	
22	DR1	Value LSB	27h	
23	DR1	Value	04h	
24	DR1	Value (= 28504,27 m^3)	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

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		
14	Access No.	Transmission counter	1Fh	1Fh		
15	Status	M-Bus state contents errors and alerts	00h	00h		
16	Config.word	NNNNCCHHb (2 encr. blocks)	00h	20h		
17	Config.word	BAS0MMMMb (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		
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)

		OMS M-Bus frame	Water meter example	
Byte No	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	Config.word	no Encryption	00h	
19	Config.word	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 ℃
Return temperature	25,1 ℃
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

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	Config.word	NNNNCCHHb (3 encr. blocks)	00h	30h	
17	Config.word	BASOMMMMb (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℃)	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℃)	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)

		OMS M-Bus frame	Heat meter example	
Byte No	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	Config.word	no Encryption	00h	
19	Config.word	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℃)	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℃)	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 ℃

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

ACC-NR (wM-Bus)

		OMS wM-Bus frame	cooling meter -> MUC		
Byte No	Field Name	Content	Bytes [hex]	Bytes [hex]	
			plain	AES coded	
1	L Field	Length of data (46 bytes)	16h	16h	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		11h	11h	
12	CRC 1		71h	71h	
13	CI Field	8Bh means 12 bytes header	8Bh	8Bh	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	FFh	FFh	
23	Status	M-Bus state contents errors and alerts	04h	04h	
24	Config.word	NNNNCCHHb (no encryption)	00h	00h	
25	Config.word	BAS0MMMMb (unidir.)	00h	00h	
26	CRC 2		B4h	B4h	DLL
27	CRC 2		18h	18h	

SND-NR (wM-Bus)

		OMS wM-Bus frame	Heat cost allocator example			
Byte No	Field Name	Content	Bytes [hex]	Bytes [hex]		
			plain	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	Config.word	NNNNCCHHb (1 encr. block)	00h	10h		
25	Config.word	BAS0MMMMb (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	
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)

		OMS M-Bus frame	HCA example			
Byte No	Field Name	Content	Bytes [hex]	Bytes [hex]		
			plain	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	Config.word	NNNNCCHHb (1 encr. block)	00h	10h		
19	Config.word	BAS0MMMMb (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

SND-NR (wM-Bus + SML-Protocol)

		OMS wM-Bus frame	electricity meter example		
Byte No	Field Name	Content	Bytes [hex]	Bytes [hex]	
			plain	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	Config.word	NNNNCCHHb (11 encr. blocks)	00h	B0h	
17	Config.word	BASOMMMMb (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		
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	AES-Encrypted Block 11	
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)

		OMS M-Bus frame	electricity meter	
Byte No	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	Config.word	no Encryption	00h	
19	Config.word	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 000000000000012345678

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	
14	Access No.	Transmission counter	01h	01h	
15	Status	M-Bus state contents errors and alerts	00h	00h	
16	Config.word	NNNNCCHHb (3 encr. blocks, static tlg.)	08h	38h	
17	Config.word	BAS0MMMMb (bidir., RX off, AES)	80h	85h	
18	AES-Verify	Encryption verification	2Fh	C8h	AES-Encrypted Block 1
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		
50	DR5	LVAR (=33 byte text string)	21h	31h		
51	DR5	Value LSB	38h	54h		
52	DR5	Value (= 000000000000012345678)	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)

		OMS wM-Bus frame	MUC -> Gas 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	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	Config.word	NNNNCCHHb	00h	00h	
25	Config.word	BAS0MMMMb (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 SND-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 acknowledge telegram indicates an application error during the 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	Config.word	NNNNCCHHb (1 encr. block)	00h	10h		
25	Config.word	BAS0MMMMb (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	96h	DLL	
30	CRC 2		61h	75h		
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]	Bytes [hex]	
			plain	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	Config.word	NNNNCCHHb	00h	00h	
25	Config.word	BAS0MMMMb (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]	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		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	Config.word	NNNNCCHHb	00h	00h	
25	Config.word	BAS0MMMMb, (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]	Bytes [hex]		
			plain	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	Config.word	NNNNCCHHb (1 encr. block)	10h	10h		
17	Config.word	BAS0MMMMb, (bidir.,RX off; AES)	85h	85h		
18	AES-Verify	Encryption verification	2Fh	FDh	AES-Encrypted Block 1	Application layer
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		
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 alternatively …

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 (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)	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	Application Error with 4 bytes header	6Eh	6Eh	APL	
14	Access No.	Transmission counter	02h	02h		
15	Status	M-Bus state “any application error”	02h	02h		
16	Config.word	NNNNCCHHb (1 encr. block)	10h	10h		
17	Config.word	BAS0MMMMb, (bidir.,RX off; AES)	85h	85h		
18	AES-Verify	Encryption verification	2Fh	9Ah		AES-Encrypted Block 1
19	AES-Verify	Encryption verification	2Fh	88h		
20	Error Code	Decryption key fails	20h	5Ch		
21	Dummy	Fill byte due to AES	2Fh	B5h		
22	Dummy	Fill byte due to AES	2Fh	62h		
23	Dummy	Fill byte due to AES	2Fh	7Eh		
24	Dummy	Fill byte due to AES	2Fh	95h		
25	Dummy	Fill byte due to AES	2Fh	B7h		
26	Dummy	Fill byte due to AES	2Fh	68h		
27	Dummy	Fill byte due to AES	2Fh	7Ch		
28	Dummy	Fill byte due to AES	2Fh	5Ah		
29	CRC 2		9Eh	ECh	DLL	
30	CRC 2		7Fh	BDh		
31	Dummy	Fill byte due to AES	2Fh	F8h		
32	Dummy	Fill byte due to AES	2Fh	1Fh		
33	Dummy	Fill byte due to AES	2Fh	5Fh		
34	Dummy	Fill byte due to AES	2Fh	E0h		
35	Dummy	Fill byte due to AES	2Fh	13h		
36	CRC 3		25h	DDh	DLL	
37	CRC 3		EEh	74h		

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)	40h	40h	
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		A9h	A9h	
12	CRC 1		80h	80h	
13	CI Field	MUC -> Meter (long header)	80h	80h	Application layer (APL)
14	Ident.Nr.	Serial No LSB (BCD)	44h	44h	
15	Ident.Nr.	Serial No (BCD)	33h	33h	
16	Ident.Nr.	Serial No (BCD) (=12345678)	22h	22h	
17	Ident.Nr.	Serial No MSB (BCD)	11h	11h	
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	Config.word	NNNNCCHHb	00h	00h	
25	Config.word	BAS0MMMMb, (bidir., RX on, no encr.)	C0h	C0h	
26	CRC 2		1Eh	1Eh	DLL
27	CRC 2		80h	80h	