netbeheer nederland

P2 Companion Standard

Dutch Smart Meter Requirements

Date:	**March 14th, 2014**
Version:	**4.2.2**
Status:	**Final**

CONTENTS

1 INTRODUCTION

1.1 Scope

This document provides a companion standard for an Automatic Meter Reading (AMR) system for electricity, thermal, (heat & cold), gas, water and hot water meters. The scope of this standard is on:

- Residential electricity meters
- Residential thermal (heat & cold) meters
- Residential gas meters
- Residential water meters

This companion standard focuses on the P2 interface for Gas, Thermal (heat / cold) and Water meters.

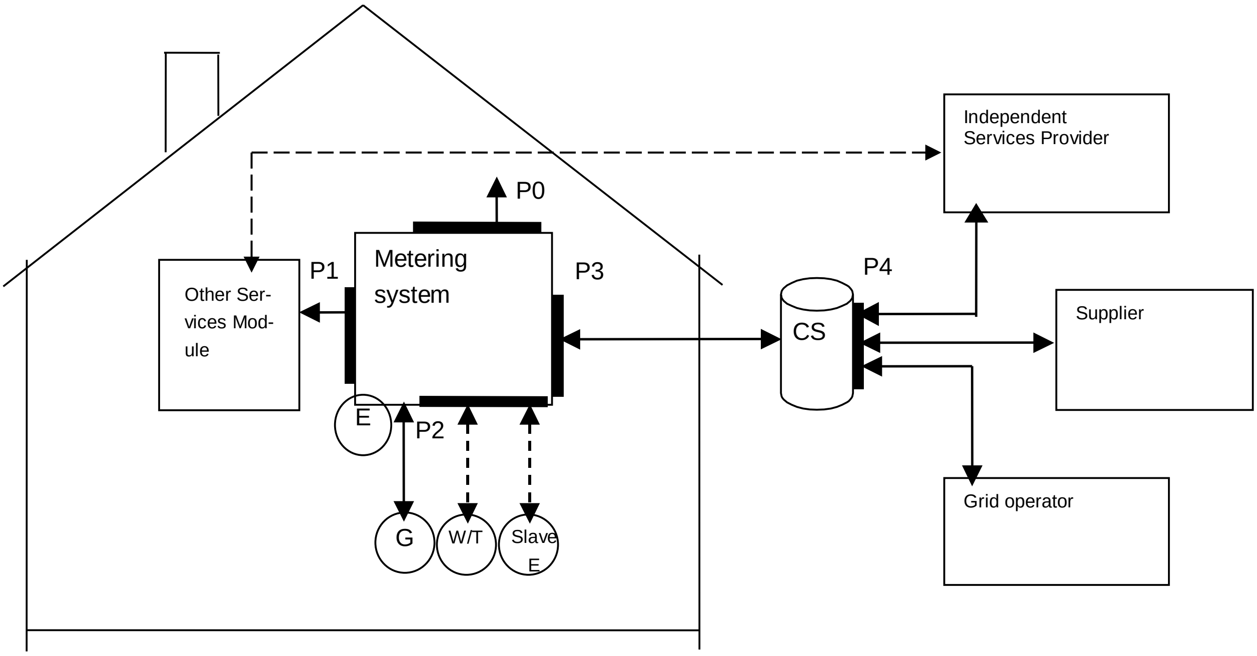


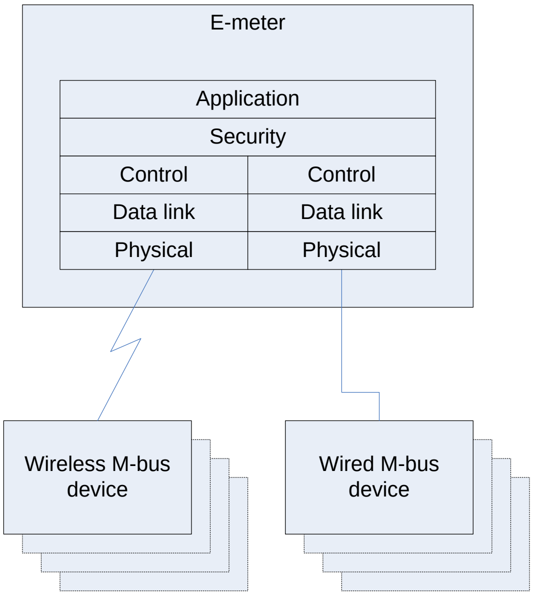
Figure 1: Meter interfaces overview.

The goal of this companion standard is to reach an open, standardized protocol implementation and functional hardware requirements related to the communication between several types of meter and an electricity meter. The features described as normative in the EN 13757 documents (ref section 1.3) need to be implemented unless specified otherwise in this document.

This companion standard is the result of a combined effort of the major Dutch grid operators.

1.2 System architecture

This companion standard focuses on the communication between E-meters that are connected to the Central System (CS) and the M-Bus devices that are connected to that meter (including Slave E-meter). This communication is based on the M-Bus References to the M-Bus standard that are included in section 1.3. This companion standard only includes deviations, clarifications or additions to the standard as defined in the relevant standard documents.



Both wired and wireless communication is supported. Wired communication is described in EN 13757-2. For wired communication the electricity meter functions as the communication master, the M-Bus devices function as communication slaves.
Wireless is described in EN 13757-4. For wireless communication the electricity meter functions as Other device according to M-Bus terminology while the wireless M-Bus device initiates communication and functions as Meter.

The electricity meter will gather and store information from all connected M-Bus devices and makes this information available to the CS.

The maximum number of M-Bus devices associated with a single E-Meter is four. This includes all wired and wireless M-Bus devices. The data requirements of the CS are based on NTA 8130 (ref. section 1.3).

The payload of communication messages between Electricity meter and M-Bus devices must be encrypted whenever the standard supports this. By exception: During installation there may be a short period of time where some messages are not encrypted

1.3 Normative references

The following standards are referred to in this company standard. For undated references the latest edition applies.

EN 13757-2:2004	Communication systems for and remote reading of meters – Part 2: Physical and link layer
EN 13757-3 Draft version January 2011	Communication systems for and remote reading of meters – Part 3: Dedicated application layer
EN 13757-4 Draft version January 2011	Communication systems for meters and remote reading of meters - Part 4: Wireless meter readout (Radio meter reading for operation in the 868 MHz to 870 MHz SRD band)
NTA 8130 NL:2007	Netherlands Technical Agreement -“Minimum set of functions for metering of electricity, gas and thermal energy for domestic customers”
DLMS Blue book 10th edition	COSEM Identification System and Interface Classes
FIPS-197	ADVANCED ENCRYPTION STANDARD (AES), published by the National Institute of Standards and Technology (NIST), USA.
AmvB	Algemene maatregel van Bestuur “Besluit op afstand uitleesbare meetinrichtingen”

Table 1-3: Normative References

Functional requirements for the metering system are defined in the NTA Requirements document (NTA 8130:2007).

1.4 Document structure

The information in this document is structured according to communication medium (wired or wireless and the various communication layers as depicted below.

	Wired	Wireless
Application: Data structures, data types, actions	EN 13757-3	
Encryption	EN 13757-3	
Control: message flow	EN 13757-2	EN 13757-4
Data Link: transmission parameters, addressing, data integrity	EN 13757-2	EN 13757-4
Physical: cable, bit representation, bus extensions, topology, electrical specifications.	EN 13757-2	EN 13757-4

Starting with the application level, each level defines layer specific header and trailer fields that must be added to the message before it can be send.

Note that the order of the detailed description of each layer is bottom up, so the Physical layer is described first. In the appendix B various message examples are given.

2 PHYSICAL LAYER

The physical layer of the P2 port is either wired or wireless and are described below.

2.1 Wired connection

The wired P2 port uses the M-Bus physical layer of EN 13757-2 (twisted pair baseband). The wired M-Bus can be used to power the M-Bus device (slave). One slave device may use a maximum mark current of four unit loads. The specification for a unit load (each unit load is 1.5 mA) is given in EN 13757-2. The maximum number of slaves is four. The physical layer shall support a fixed baud rate of 2400 Baud. Table 1 gives a summary of these parameters.

Baud rate	2400 Baud
Max. number of M-Bus slaves	4
Max. current per M-Bus slave	6 mA (4*1,5 mA)

Table 1: Wired M-Bus Physical Interface Configuration.

2.2 Wireless connection

The wireless P2 port uses the M-Bus physical layer of EN 13757-4 (RF = radio frequency). The communication shall be established according to the bidirectional sub-mode T2. In this mode of operation, the M-Bus device regularly transmits the readout value after which it is able to receive a response from the E-meter for a very short period. Then the M-Bus device turns into sleep mode until its next transmission.

The T2 parameters are defined in EN13757-4 and are all mandatory. Since the wireless M-Bus device will be deployed in very difficult situations, the highest performance class is demanded. The transmit power shall be according to performance class H_T (+5 dBm transmitter for the M-Bus device, +8 dBm transmitter for the E-meter). The receiver sensitivity and blocking performance shall be according to performance class H_R (min. sensitivity of -100 dBm).

When the M-Bus device is the transmitter, the header of the preamble sequence shall contain n≥19 01-patterns before the synchronisation word (0000111101), as specified in the EN13757-4 standard. However, the E-meter shall already meet the receiver performance requirements with a maximum of 19 01-patterns. The E-meter may support the “capture effect” and detect other (new or stronger) transmissions based on the part of the preamble header while receiving another frame.

When the E-meter is the transmitter, the header of the preamble sequence shall contain n≥15 01-patterns before the synchronisation word (0001110110), as specified in the EN13757-4 standard. However, the M-Bus device shall already meet the receiver performance requirements with a maximum of 15 01-patterns.

3 DATA LINK LAYER

For both wired and wireless the Link transmission procedures of EN 60870-5-2 are used, but the frame format classes differ for both media. The following two sections describe the media specific usage of the link layer.

3.1 Wired Connections

For the wired M-Bus link layer the format class FT1.2 of EN 60870-5-1 and a telegram structure for a frame with variable length according to EN 60870-5-2 shall be used, see Table 2: Frame format FT1.2Table 2. This frame format includes a length field (L), a control field (C) and an address field (A). Refer to EN 13757-2 for field definitions in the protocol header.

Field		Remark
	68h	Start Character
	L	Length
	L	Length
	68h	Start Character
	C	Control field
	A	Primary M-Bus address
	Link user data	Variable length data block
	Checksum	Specified in EN 60870-5-1
	16h	Stop character

Table 2: Frame format FT1.2

3.1.1 Length field (L)

The length field specifies the message length in bytes, excluding length and CRC fields The maximum length of a single telegram is 255 bytes.

3.1.2 Control field (C)

The control field specifies the frame type. In deviation from EN 13757-2, the allowed telegram types are: SND_NKE, REQ_UD2, SND_UD, RSP_UD, REQ_UD1, REQ_SKE, RSP_SKE. The last three telegram types are mandatory according to M-Bus, but not used in the DSMR.

The frame count bit (FCB) of the C-Field is ignored. At the Control Layer, the Access Number shall be used to detect communication failures.

3.1.3 Address field (A)

One byte addressing is used for primary addressing of slaves in the range of 1 to 250. Address values higher than 250 shall be ignored by the slaves. Secondary addressing (A=253) is not allowed.

3.1.4 Baud rate

In deviation from EN 13757-2, the baud rate settings for wired configurations are fixed, at all times and in any situation, to settings of Table 3. This applies also after reset of the communication link.

Baud rate	2400
Parity	Even
Data Bits	8
Stop Bit	1

Table 3: Wired M-Bus Interface Configuration

3.1.5 Master/slave

The E- meter is the master device, meaning that all communication is initiated from it. An alarm of a connected M-Bus device will only be indicated during the next reading of the device. It will not push an immediate alarm.

3.2 Wireless Connections

For the wireless M-Bus link layer the format class FT3 of EN 60870-5-1 and a telegram structure for a frame with variable length according to EN 60870-5-2 shall be used. Note that the Start bytes 05h 64h are replaced by the Preamble Chip Sequence as described in EN 13757-4. This frame format includes a length field (L), a control field (C) and an address field (A). The general format A of EN 13757-4 shall be used for the protocol header, see Table 4, with deviations as discussed in the following.

Field		Remark
	PL	Preamble
	L	Length
	C	Control field
	M	Manufacturer ID
	A	Address field of the sending Meter
	Checksum	Specified in EN 60870-5-1
	Link user data	Variable length data block
	Checksum	Specified in EN 60870-5-1
	…	…
	Link user data	Variable length data block
	Checksum	Specified in EN 60870-5-1
	‘01’b or ‘10’b	Postamble

Table 4: Frame format FT3 (general format A).

3.2.1 Length field (L)

The length field specifies the message length in bytes, excluding length and CRC fields. The maximum length of a single telegram is 255 bytes.

3.2.2 Control field (C)

The control field specifies the frame type. In deviation from EN 13757-4, the allowed telegram types are: SND_NKE, REQ_UD2, RSP_UD, SND_UD, SND_NR, ACK, SND_IR and CNF_IR. Not allowed are REQ_UD1, ACC_NR and ACC_DMD.
The frame count bit (FCB) of the C-Field is ignored. At the Control Layer, the Access Number shall be used to detect communication failures.

3.2.3 Manufacturer Identification field (MAN)

An 2 byte field is used to identify the manufacturer as specified in clause 5.6 of EN 13757-3
.

3.2.4 Address field (A: ID | VER | DEV)

An 6 bytes address field is used to identify the sender (source) as defined in EN 13757-4 Annex E. The A-field shall be generated as a concatenation of Identification Number (ID-field: 4 octets), Version identification (VER-field: 1 octet) and Device Type identification (DEV-field, 1 octet), all specified in EN 13757-3. See also Note 1.

If the M-Bus device is the sender, the address at the Data Link Layer and the address at the Control Layer will be the same Meter address (LLA and ALA respectively in EN 13757-4 Annex E).

In deviation from EN 13757-4, this address field shall be ignored by the M-Bus device if the E-meter is the sender (see Note 2); the M-Bus device (being the receiver or target) will use the address field from the Control Layer to identify the target device (see the section Control Layer). This implies that for the E-meter, the Data Link Layer address (LLA) may be left empty (all zero).[1, 2]

3.2.5 Timing

EN 13757-4 details about various timing aspects at Data Link Layer level which will be further specified in this section.

[1] EN 13757-4 allows for different addressing of the meter and the RF module (radio). In this document it is assumed that the radio is integrated with the equipment (E-meter and M-Bus device) and only a single address is defined.

[2] This requirement is adopted to allow a transparent E-meter exchange without additional configuration of the M-Bus device with an E-meter address.

In installation mode, the M-Bus device shall transmit SND_IR messages every minute during 60 minutes as long as the M-Bus device does not receive an appropriate response (CNF_IR) from the designated E-meter. After 60 minutes, it continues transmitting installation messages (SND_IR) once every hour until reception of an appropriate response (CNF_IR) from the designated E-meter.

The transmission of the regular user data messages (SND_NR with billing data) from the M-Bus device shall have a randomized timing, using the synchronous transmission algorithm. In deviation from EN 13757-4, the nominal transmission interval T_{nom} is set to 3600 s (for T mode, EN 13757-4 specifies a maximum T_{nom} of 15 min). Care must be taken so that the random transmission interval fits within the 10 minutes window after the whole hour that is allowed for M-Bus transmissions (requirement M4.5.7 in the DSMR Main document), for instance by applying an appropriate offset. The hourly transmission shall always transmit the new hourly meter reading and never starts before the meter data that needs to be transmitted is available.
The Control Layer shall support the required Access Number initialisation and increments. The sync-bit in the Configuration Field (see next section) of the M-Bus device shall be set.

To get access to the M-Bus device, both the E-meter and the M-Bus device shall support the Frequent Access Cycle and the related timing for T-mode. The M-Bus device shall indicate the accessibility as Limited Access (bit 15 (B) = 1 and bit 14 (A) = 0 in the Configuration word). The E-meter (as sender) shall set the Configuration word bits 15 (B) and 14 (A) to 0.

4 CONTROL LAYER

The Control Layer is inserted here to specify and clarify how the message flows are managed. This layer is not a formal part of the M-Bus series (EN 13757), but it combines the control field (C-field) of the Data Link Layer, the control information field (CI-field) of the Transport Layer and related elements to control exchange of messages between the E-meter and the M-Bus device. The Control Layers for wired and wireless are different but have common elements. The common elements are specified first, the respective differences in the following sections.

4.1 Allowed control elements

The following two tables define the messages and their response that shall be used for the message transactions. Table 5 contains the C-field and CI-field control elements for wired connections. [Table 6] contains the C-field and CI-field control elements for wireless connections. For security reasons, all combinations of C and CI codes that are not described in this section shall be rejected (meaning: no further processing of the message).

WIRED M-Bus connection				
Purpose	Initiator	Direction data	Message	Response
Normalisation message: reset link	E-meter	<none>	SND_NKE C=40h; CI=< >	$E5h <single char>
Meter data message: billing data, status, version	E-meter	M-Bus device to E-meter	REQ_UD2 C=5Bh; CI=< >	RSP_UD C=08h; CI=72h
Control message: readout list	E-meter	E-meter to M-Bus device	SND_UD C=53h; CI=5Ah	$E5h <single char>
Control message: clock synchronisation	E-meter	E-meter to M-Bus device	SND_UD C=53h; CI=6Ch	$E5h <single char>
Unencrypted message: set M-Bus address, set key	E-meter	E-meter to M-Bus device	SND_UD C=53h; CI=51h	$E5h <single char>
Time critical data message: not used, but standard	E-meter	M-Bus device to E-meter	REQ_UD1 C=5Ah; CI=< >	$E5h <single char>
Status request message: not used, but standard	E-meter	<none>	REQ_SKE C=59h; CI=< >	RSP_SKE C=xBh; CI=< >

Table 5: Control Layer for wired connections with allowed C-field and CI-field combinations.

WIRELESS M-Bus connection				
Purpose	Initiator	Direction data	Message	Response
Normalisation message: reset link, stop FAC	E-meter	<none>	SND_NKE C=40h; CI=80h	<none>
Meter data message: billing data, status, version	M-Bus device	M-Bus device to E-meter	SND_NR C=44h; CI=7Ah	<none>
On-demand data message: billing data, status	E-meter	M-Bus device to E-meter	REQ_UD2 C=5Bh; CI=80h	RSP_UD C=08h; CI=7Ah
Control message: readout list	E-meter	E-meter to M-Bus device	SND_UD C=53h; CI=5Bh	ACK C=00h; CI=8Ah
Control message: clock synchronisation	E-meter	E-meter to M-Bus device	SND_UD C=53h; CI=6Ch	ACK C=00h; CI=8Ah
Unencrypted message: set key (conf. word = 00h)	E-meter	E-meter to M-Bus device	SND_UD C=53h; CI=5Bh	ACK C=00h; CI=8Ah
Installation message: broadcast and registration	M-Bus device	<none>	SND_IR C=46h; CI=7Ah	CNF_IR C=06h; CI=80h

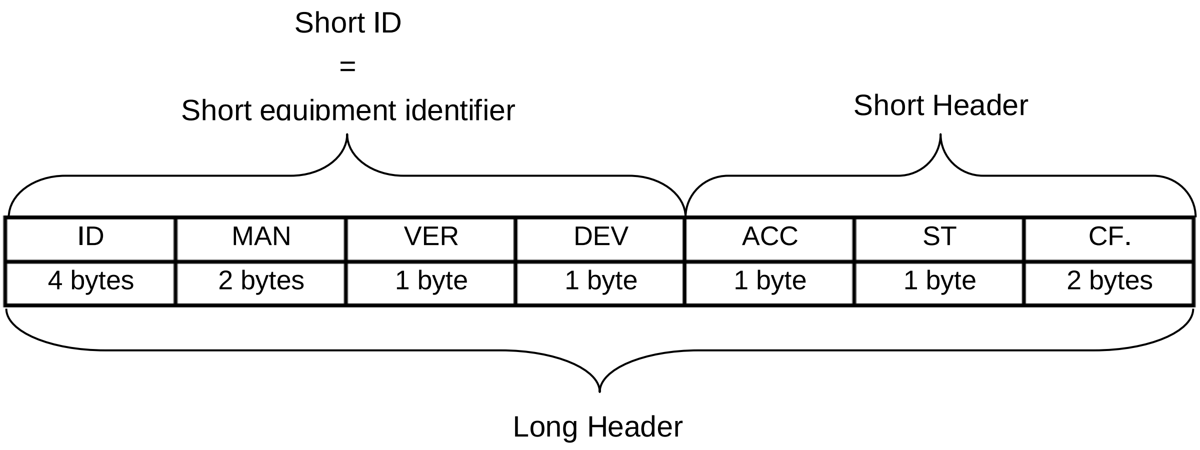
Table 6: Control Layer for wireless connections with allowed C-field and CI-field combinations

4.2 Common control elements

4.2.1 Data Headers

Depending on the CI code, the message shall contain a short or a long header as is specified in EN 13757-3, see [Figure 2]. Specifically, CI codes 5Ah, 7Ah and 8Ah shall use a short data header and CI codes 5Bh, 72h and 80h shall use a long data header. The long data header address is in the format of the short equipment identifier.

Note: The CI-code 51h contains no header information, hence no address.



ID	MAN	VER	DEV	ACC	ST	CF.
4 bytes	2 bytes	1 byte	1 byte	1 byte	1 byte	2 bytes

Figure 2: Definition of long header, short header and Short ID.

4.2.2 Short Equipment Identifier (Short ID: ID | MAN | VER | DEV)

The M-Bus device shall use the concatenation of Identification Number (ID-field: 4 octets), Manufacturer identification (MAN-field: 2 octets), Version identification (VER-field: 1 octet) and Device Type identification (DEV-field, 1 octet), all specified in EN 13757-3, as short equipment identifier (Short ID), see [Figure 2]. The Short ID is added because the encrypted full equipment identification is hidden during certain installation processes. The uniqueness of the Short ID (in the Netherlands) shall be guaranteed by the manufacturer over the lifetime of the meter type. The Identification Number is derived from the 17 digits Equipment Identifier. The last 8 digits of the 10 digits serial number within the Equipment Identifier are used as Identification Number and packed in 4 bytes BCD format.

Notice that for wireless, the link layer address (see 3.2.4) is similar but not identical to the Short ID because the MAN en ID fields are swapped. Since the fields are stored in individual P3 objects of the E-meter, this should be no issue for the central system. In addition, if the E-meter sends a message, its address will be ignored by the M-Bus device. Hence, the Short ID is not specified for the E-meter.

4.2.3 Version: DSMR compliancy level

The P2 interface must support remote reading of the DSMR compliance level. The version field in the fixed header is used to transfer this information from the M-Bus device.
The field version specifies the Major and Minor version number of the DSMR standard that the meter complies to. The Major version is stored in the high nibble; the minor version number is stored in the low nibble of the version field.

Example: meters that comply with version 4.2 of the DSMR should use 42h as the DSMR compliance level in the header of each message.

4.2.4 Access Nr (ACC)

The access number in the data header (ACC-field) will be maintained by the M-Bus device as specified in EN 13757-3 section 5.9. As stated the Access Number of the M-Bus device shall be initialised by a random number which will be independent for each M-Bus device.

4.2.5 Status (ST)

The status byte in the header is not protected and vulnerable for compromising the communication. Therefore it is not used and its value is set to 0. The status can be retrieved using the DIF/VIF combination described in 6.3.3.

4.2.6 Configuration word (CW)

MSBit 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	Bit 0
Bidirectional communicationn	Accessibility	Synchronized	Reserved	Mode bit 3	Mode bit 2	Mode bit 1	Mode bit 0	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

This is a general Configuration word (CW-field) and coded according to EN13757-3, see Figure above. The usage for wired and wireless will be different with common usage of the "MMMM" and "NNNN" bits for encryption information (see section 5.1). For wired, all bits except "MMMM" and "NNNN" shall be set to "0" for both the E-meter and the M-Bus device. For wireless, the M-Bus device shall set the 15 (B) and bit 13 (S) to "1", and the remaining bits except "MMMM" and "NNNN" to "0". For all synchronized messages, being only SND_NR messages (C-field 44h), bit 13 (S) will be set to "1". For all other, asynchronous messages, bit 13 (S) will be set to "0".

The wireless E-meter shall set all bits except "MMMM" and "NNNN" to "0" The usage of the "MMMM" and "NNNN" bits are part of the Encryption Layer as specified in the section 5.

4.3 Wired Connections

During standard operation the E-meter collects the consumption data by polling the M-Bus device at the available device addresses. Polling should be on an hourly basis. The following sections details the control layer of the various message types for wired connections. See Table 5 for reference to message types.

4.3.1 Normalisation message

The E-meter initiates communication by sending a short frame to the specific M-Bus device: SND_NKE

Field	Hex	Remark
Start Character	10h	Short format
C-Field	40h	SND_NKE
A-Field	A-0	Primary Address of M-Bus slave
Checksum	CS-0	Sum of A and C fields, two least significant Hex digits
Stop Character	16h	Always 16H

The response of an M-Bus device:

Field	Hex	Remark
Single character	E5h	The slave returns SCC (single control character)

The message SND_NKE can be also be used for detecting new devices on M-Bus address zero (see installation procedure in [section 8]). After receiving the E5h reply, the E-meter can identify the M-Bus device by requesting the device with a REQ_UD2. The slave shall answer with a RSP_UD (see next section).

4.3.2 Meter data message

The E-meter requests for data by sending a short frame: REQ_UD2.

Field	Hex	Remark
Start Character	10h	Short format
C-Field	5Bh	REQ_UD2
A-Field	A-0	Primary Address of M-Bus slave
Checksum	CS-0	Sum of A and C fields, two least significant Hex digits
Stop Character	16h	Always 16H

The M-Bus device shall respond with a long format frame: RSP_UD

Field	Hex	Remark
Start	68h	Start byte Long Telegram
L	L-0	Length xx Bytes
L	L-0	Length xx Bytes
Start	68h	Start byte
C	08h	Send data from slave to master
A	A-0	Primary Address of M-Bus slave
CI	72h	Answer of variable length
Identification Number	ID-0	Ident Number, e.g. 12345678 in BCD
	ID-1	
	ID-2	
	ID-3	
Manufacturer ID	MAN-0	Manufacturer ID
	MAN-1	
Version	VER-0	DSMR Protocol version, e.g. 42h (=4.2)
Device type	DEV-0	Device type, refer to EN 13757-3 for codes
Access Nr	ACC-0	Access Counter
Status	ST-0	Not used
Configuration Word	CW-0	Encryption information
	CW-1	
Encrypted Variable Data Blocks (Records) (ref section 6.4)		
CS	CS-0	Checksum
Stop	16h	Stop

Remarks

- The long 12 byte header (refer to 4.2.1) is mandatory in variable length data blocks (further specified in 6.4)
- This is a template frame, mainly to indicate the mandatory fields. There are no variable blocks inserted here; the length field depends on this content.

- When there is no User key for encryption available (i.e. User key is equal to zero, e.g. at installation time), the same message type shall be used to transmit meter data messages on request with Configuration word equal to zero.

4.3.3 Control message

The E-meter sends control and configuration information to the specific M-Bus device with SND_UD. For encrypted messages CI=5Ah with short header is used. Unencrypted messages are described in the following section.

Field	Hex	Remark
Start	68h	Start byte Long Telegram
L	L-0	Length xx Bytes
L	L-0	Length xx Bytes
Start	68h	Start byte
C	53h	SND_UD
A	A-0	Primary Address of M-Bus slave
CI	5Ah	Send user data of variable length
Access Nr	ACC-0	Access Counter
Status	ST-0	Not used
Configuration Word	CW-0	Encryption information
	CW-1	
Encrypted Variable Data Blocks (Records) (ref section 6.4)		
CS	CS-0	Checksum
Stop	16h	Stop

The response of an M-Bus device:

Field	Hex	Remark
Single character	E5h	The slave returns SCC (single control character)

4.3.4 Clock synchronisation message

The E-meter sends the clock synchronisation control information with a specific SND_UD. Both for encrypted and unencrypted messages CI=6Ch with long header is used, distinguished by the Encryption Method Code (see section 5.1). Important: the unencrypted messages are only allowed and accepted by the M-Bus device when the User key is not set (equal to zero), typically during installation.

Field	Hex	Remark
Start	68h	Start byte Long Telegram
L	L-0	Length xx Bytes
L	L-0	Length xx Bytes
Start	68h	Start byte
C	53h	SND_UD
A	A-0	Primary Address of M-Bus slave
CI	6Ch	Time Sync to device

Field		Hex	Remark
Short ID of M-Bus device	Identification Number	ID-0	Ident Number, e.g. 12345678 in BCD (of target M-Bus device)
		ID-1	
		ID-2	
		ID-3	
	Manufacturer ID	MAN-0	Manufacturer ID (of target M-Bus device)
		MAN-1	
	Version	VER-0	DSMR Protocol version, e.g. 42h (=4.2) (of target M-Bus device)
	Device type	DEV-0	Device type, refer to EN 13757-3 for codes (of target M-Bus device)
Access Nr		ACC-0	Access Counter (of E-meter)
Status		00h	Not used
Configuration Word		CW-0	Encryption information
		CW-1	
Time Sync to device, either encrypted or unencrypted (ref section 6.2.1)			
CS		CS-0	Checksum
Stop		16h	Stop

The response of an M-Bus device:

Field	Hex	Remark
Single character	E5h	The slave returns SCC (single control character)

4.3.5 Unencrypted message

Specific control information, in specific circumstances, may be transmitted with an unencrypted message type. The E-meter sends this control and configuration information to the specific M-Bus device with SND_UD using CI=51h without a header.

Field	Hex	Remark
Start	68h	Start byte Long Telegram
L	L-0	Length xx Bytes
L	L-0	Length xx Bytes
Start	68h	Start byte
C	53h	SND_UD
A	A-0	Primary Address of M-Bus slave
CI	51h	Send user data of variable length
Unencrypted Variable Data Blocks (Records) (ref section 6.4)		
CS	CS-0	Checksum
Stop	16h	Stop

The response of an M-Bus device:

Field	Hex	Remark
Single character	E5h	The slave returns SCC (single control character)

4.4 Wireless Connections

Wireless messages between the E-meter and the M-Bus device shall be exchanged in T2-mode of the wireless M-Bus protocol according to the specification EN 13757-4. This means that for meter data messages, the M-Bus device behaves as a primary station (described in EN 60870-5-2) and transmits periodically unacknowledged messages with billing data to the E-meter. The average period is T_{NOM} with randomized variation as discussed in section 3.2.5 on Timing. The message type is SND_NR (Send / No Reply) with a short address header. If the E-meter has a command, a request or data to send to the M-Bus device, it shall use the so-called Frequent Access Cycle (FAC) method (section 10.6.3.2 in EN 13757-4). It provides the E-meter a short access window (response delay t_{RO} specified in EN 13757-4) after every transmission of the M-Bus device until the FAC reached the maximum number of transmissions (6).

For the FAC the following applies

- maximum 6 cycles = maximum 6 transmissions from M-Bus device during FAC
- FAC time out = max 6 transmissions, no time specification
- FAC transmission delay = not specified; N=2, 3, 4 or 5

The E-meter is implemented efficiently if it assumes N=5. Otherwise it may assume failed transmissions and starts repetitions too early. This is not required and other implementations are allowed as long as it will not impair interoperability.

The wireless message transactions timing diagram is summarized in Figure 3 and detailed in the subsequent sections. The figure shows two sides of the communication channel. One is the E-meter with the symbolic data link layer address (LLA) E-MTR and the other is the M-Bus device with the symbolic application layer address (ALA; actually Transport layer address) being equal to the data link layer address (LLA) M-DEV. The vectors in the message exchange timing diagram signify directional messages with the data link layer message type (with C-field and data link layer address), the control information of the application layer followed by the application layer address (if applicable) and the access number (ACC). The access number values are examples to show the behaviour. The EN 13757 specifications are ambiguous on the behaviour of the access number[3]. This document follows the EN 13757-4 specification and asynchronous transmissions (e.g. the FAC) starts with a newly initiated ACC that is incremented every subsequent asynchronous transmission of the M-Bus device. The other content is fixed and depending only on the type of message and its origin. The data link layer address shall always be the address of the sender, but as stated in section 3.2.4

[3] EN-13757-3 states “For every asynchronous transmission between two synchronous telegrams the meter shall use the access number from the last synchronous transmission.” - i.e. the access number is frozen during the frequent access cycle. Annex E of EN 13757-4 shows an incrementing ACC.

(address field for wireless): the data link layer address of the E-meter is not specified and shall be ignored by the M-Bus device.

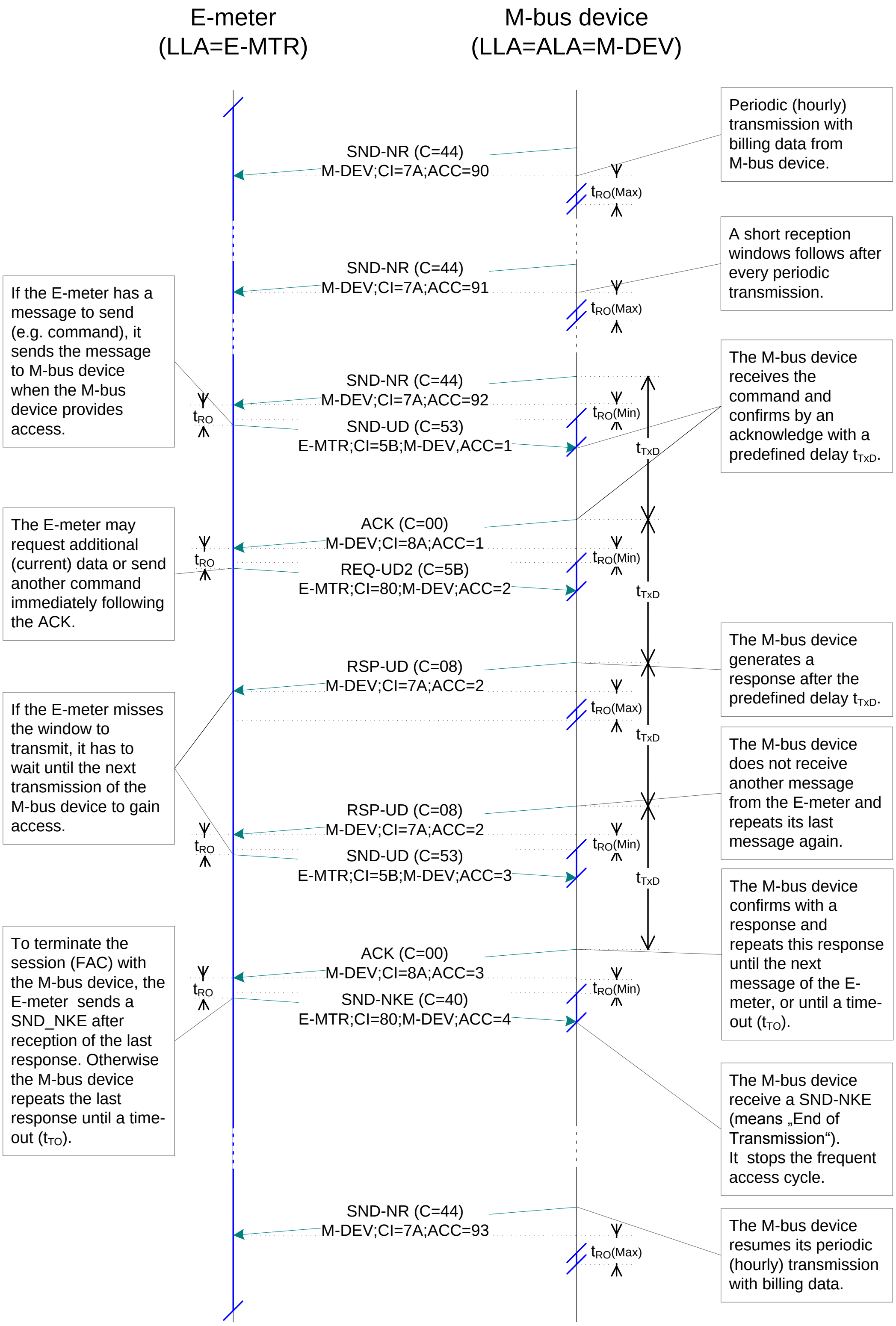

E-meter
(LLA=E-MTR)
M-bus device
(LLA=ALA=M-DEV)
SND-NR (C=44)
M-DEV;CI=7A;ACC=90
t_{RO}(Max)
Periodic (hourly) transmission with billing data from M-bus device.
SND-NR (C=44)
M-DEV;CI=7A;ACC=91
t_{RO}(Max)
A short reception windows follows after every periodic transmission.
If the E-meter has a message to send (e.g. command), it sends the message to M-bus device when the M-bus device provides access.
t_{RO}
SND-NR (C=44)
M-DEV;CI=7A;ACC=92
SND-UD (C=53)
E-MTR;CI=5B;M-DEV,ACC=1
t_{RO}(Min)
t_{TxD}
The M-bus device receives the command and confirms by an acknowledge with a predefined delay t_{TxD}.
The E-meter may request additional (current) data or send another command immediately following the ACK.
t_{RO}
ACK (C=00)
M-DEV;CI=8A;ACC=1
REQ-UD2 (C=5B)
E-MTR;CI=80;M-DEV;ACC=2
t_{RO}(Min)
t_{TxD}
RSP-UD (C=08)
M-DEV;CI=7A;ACC=2
t_{RO}(Max)
t_{TxD}
The M-bus device generates a response after the predefined delay t_{TxD}.
If the E-meter misses the window to transmit, it has to wait until the next transmission of the M-bus device to gain access.
The M-bus device does not receive another message from the E-meter and repeats its last message again.
t_{RO}
RSP-UD (C=08)
M-DEV;CI=7A;ACC=2
SND-UD (C=53)
E-MTR;CI=5B;M-DEV;ACC=3
t_{RO}(Min)
t_{TxD}
The M-bus device confirms with a response and repeats this response until the next message of the E-meter, or until a time-out (t_{TO}).
To terminate the session (FAC) with the M-bus device, the E-meter sends a SND_NKE after reception of the last response. Otherwise the M-bus device repeats the last response until a time-out (t_{TO}).
t_{RO}
ACK (C=00)
M-DEV;CI=8A;ACC=3
SND-NKE (C=40)
E-MTR;CI=80;M-DEV;ACC=4
t_{RO}(Min)
The M-bus device receive a SND-NKE (means „End of Transmission“).
It stops the frequent access cycle.
SND-NR (C=44)
M-DEV;CI=7A;ACC=93
t_{RO}(Max)
The M-bus device resumes its periodic (hourly) transmission with billing data.

Figure 3: Timing diagram of wireless message transactions in T2-mode with short address.

4.4.1 Normalisation message

The E-meter resumes to normal operation mode (get outside frequent access cycle for instance) by sending a short frame to the specific M-Bus device: SND_NKE

Field		Hex	Remark
Preamble of physical layer			
L-field		L-0	Length xx Bytes
C-Field		40h	SND_NKE
MAN-Field of sender		M-0	Manufacturer identification of the E-meter (or 00 00h) (this will be ignored by the M-Bus device)
		M-1	
A-Field of sender		A-0	Address (or 00 00 00 00 00h) of the E-meter (this will be ignored by the M-Bus device)
		A-1	
		A-2	
		A-3	
		A-4	
		A-5	
Checksum		CS-0	2 bytes checksum for wireless FT3 format
		CS-1	
CI		80h	Transport layer without application data
Short ID of M-Bus device	Identification Number	ID-0	Ident Number, e.g. 12345678 in BCD (of target M-Bus device)
		ID-1	
		ID-2	
		ID-3	
	Manufacturer ID	MAN-0	Manufacturer ID (of target M-Bus device)
		MAN-1	
	Version	VER-0	DSMR Protocol version, e.g. 42h (=4.2) (of target M-Bus device)
	Device type	DEV-0	Device type, refer to EN 13757-3 for codes (of target M-Bus device)
Access Nr		ACC-0	Access Counter (of E-meter)
Status		00h	Not used
Configuration Word		00h	No application data, no encryption
		00h	
Checksum		CS-0	2 bytes checksum for wireless FT3 format
		CS-1	
Postamble of physical layer			

There is no response from the M-Bus device; it just accepts this message and starts the periodic transmission of the meter data message as described in the following section.

4.4.2 Meter data message

The M-Bus device transmits unsolicited meter data message without reply: SND_NR.

Field	Hex	Remark
Preamble of physical layer		
L-field	L-0	Length xx Bytes
C-Field	44h	SND_NR
MAN-Field of sender	M-0	Manufacturer identification of the M-Bus device (=sender)
	M-1	
A-Field of sender	A-0	A-field of the M-Bus device (=sender)
	A-1	
	A-2	
	A-3	
	A-4	
	A-5	
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
CI	7Ah	Transport layer with short header
Access Nr	ACC-0	Access Counter (of M-Bus device)
Status	ST-0	Not used
Configuration Word	CW-0	Encryption information + Limited Access bits set
	CW-1	
Encrypted Variable Data Blocks (Records) (ref section 6.4)		
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
Postamble of physical layer		

Remarks

- The short header is sufficient (and mandatory) since the target will always be the designated E-meter.
- This is a template frame, mainly to indicate the mandatory bits and pieces. There are no variable blocks inserted here; the length field depends on this content.
- When there is no User key for encryption available (i.e. User key is equal to zero, e.g. at installation time), the same message type shall be used to transmit meter data messages with Configuration word equal to A0h (Limited Access bits set).

4.4.3 Control message

The E-meter sends control and configuration information to the specific M-Bus device within the so-called frequent access cycle (FAC). It is started with a valid transmission from the E-meter just after a regular meter data transmission from the M-Bus device, which will then be in receive mode during a short window (t_{RO}). The valid transmission may just well be control and configuration information, sent with message type SND_UD using CI=5Bh and long header. Unencrypted messages are described in the following section.

Field		Hex	Remark
Preamble of physical layer			
L-field		L-0	Length xx Bytes
C-Field		53h	SND_UD
MAN-Field of sender		M-0	Manufacturer identification of the E-meter (or 00 00h) (this will be ignored by the M-Bus device)
		M-1	
A-Field of sender		A-0	Short ID (or 00 00 00 00 00h) of the E-meter (this will be ignored by the M-Bus device)
		A-1	
		A-2	
		A-3	
		A-4	
		A-5	
Checksum		CS-0	2 bytes checksum for wireless FT3 format
		CS-1	
CI		5Bh	Application data from E-meter to M-Bus device with long header
Short ID of M-Bus device	Identification Number	ID-0	Ident Number, e.g. 12345678 in BCD (of target M-Bus device)
		ID-1	
		ID-2	
		ID-3	
	Manufacturer ID	MAN-0	Manufacturer ID (of target M-Bus device)
		MAN-1	
	Version	VER-0	DSMR Protocol version, e.g. 42h (=4.2) (of target M-Bus device)
	Device type	DEV-0	Device type, refer to EN 13757-3 for codes (of target M-Bus device)
Access Nr		ACC-0	Access Counter (of E-meter)
Status		00h	Not used
Configuration Word		CW-0	Encryption information
		CW-1	
Encrypted Variable Data Blocks (Records) (ref section 6.4)			
Checksum		CS-0	2 bytes checksum for wireless FT3 format
		CS-1	
Postamble of physical layer			

The response of an M-Bus device is an acknowledgement: ACK

Field	Hex	Remark
Preamble of physical layer		
L-field	L-0	Length xx Bytes
C-Field	00h	ACK
MAN-Field of sender	M-0	Manufacturer identification of the M-Bus device (=sender)
	M-1	
A-Field of sender	A-0	Short ID of the M-Bus device (=sender)
	A-1	
	A-2	
	A-3	
	A-4	

Field	Hex	Remark
	A-5	
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
CI	8Ah	Transport layer with short header
Access Nr	ACC-0	Access Counter (copied from SND_UD)
Status	ST-0	Not used
Configuration Word	A0h	No application data, no encryption, with Limited Access bits set
	00h	
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
Postamble of physical layer		

Remarks

- If within the FAC (or at the start of the FAC) insufficient processing time is available after a transmission from the M-Bus device, the E-meter may use a void request with REQ_UD2 to gain time and prepare. The response is ignored, after which the true message is sent.

4.4.4 Clock synchronisation message

The E-meter sends the clock synchronisation control information with a specific SND_UD. Both for encrypted and unencrypted messages CI=6Ch with long header is used, distinguished by the Encryption Method Code (see section 5.1). Important: the unencrypted messages are only allowed and accepted by the M-Bus device when the User key is not set (equal to zero), typically during installation.

Field	Hex	Remark
Preamble of physical layer		
L-field	L-0	Length xx Bytes
C-Field	53h	SND_UD
MAN-Field	M-0	Manufacturer identification of the E-meter (or 00 00h)
of sender	M-1	(this will be ignored by the M-Bus device)
A-Field	A-0	Short ID (or 00 00 00 00 00h) of the E-meter
of sender	A-1	(this will be ignored by the M-Bus device)
	A-2	
	A-3	
	A-4	
	A-5	
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
CI	6Ch	Time Sync to device
Short ID Identification Number	ID-0	Ident Number, e.g. 12345678 in BCD
	ID-1	(of target M-Bus device)
	ID-2	
	ID-3	

Field		Hex	Remark
	Manufacturer ID	MAN-0	Manufacturer ID (of target M-Bus device)
		MAN-1	
	Version	VER-0	DSMR Protocol version, e.g. 42 (=4.2) (of target M-Bus device)
	Device type	DEV-0	Device type, refer to EN 13757-3 for codes (of target M-Bus device)
Access Nr		ACC-0	Access Counter (of E-meter)
Status		00h	Not used
Configuration Word		CW-0	Encryption information
		CW-1	
Time Sync to device, either encrypted or unencrypted (ref section 6.2.1)			
Checksum		CS-0	2 bytes checksum for wireless FT3 format
		CS-1	
Postamble of physical layer			

The response of an M-Bus device is an acknowledgement: ACK

Field	Hex	Remark
Preamble of physical layer		
L-field	L-0	Length xx Bytes
C-Field	00h	ACK
MAN-Field of sender	M-0	Manufacturer identification of the M-Bus device (=sender)
	M-1	
A-Field of sender	A-0	Short ID of the M-Bus device (=sender)
	A-1	
	A-2	
	A-3	
	A-4	
	A-5	
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
CI	8Ah	Transport layer with short header
Access Nr	ACC-0	Access Counter (copied from SND_UD)
Status	ST-0	Not used
Configuration Word	A0h	No application data, no encryption, with Limited Access bits set
	00h	
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
Postamble of physical layer		

4.4.5 On-demand data message

The E-meter may request meter data on demand from the specific M-Bus device within the FAC using REQ_UD2.

Field		Hex	Remark
Preamble of physical layer			
L-field		L-0	Length xx Bytes
C-Field		5Bh	REQ_UD2
MAN-Field of sender		M-0	Manufacturer identification of the E-meter (or 00 00h) (this will be ignored by the M-Bus device)
		M-1	
A-Field of sender		A-0	Short ID (or 00 00 00 00 00h) of the E-meter (this will be ignored by the M-Bus device)
		A-1	
		A-2	
		A-3	
		A-4	
		A-5	
Checksum		CS-0	2 bytes checksum for wireless FT3 format
		CS-1	
CI		80h	Transport layer without application data
Short ID of M-Bus device	Identification Number	ID-0	Ident Number, e.g. 12345678 in BCD (of target M-Bus device)
		ID-1	
		ID-2	
		ID-3	
	Manufacturer ID	MAN-0	Manufacturer ID (of target M-Bus device)
		MAN-1	
	Version	VER-0	DSMR Protocol version, e.g. 42h (=4.2) (of target M-Bus device)
	Device type	DEV-0	Device type, refer to EN 13757-3 for codes (of target M-Bus device)
Access Nr		ACC-0	Access Counter (of E-meter)
Status		00h	Not used
Configuration Word		00h	No application data, no encryption
		00h	
Checksum		CS-0	2 bytes checksum for wireless FT3 format
		CS-1	
Postamble of physical layer			

The M-Bus device responses with (encrypted) meter data: RSP_UD

Field	Hex	Remark
Preamble of physical layer		
L-field	L-0	Length xx Bytes
C-Field	08h	RSP_UD
MAN-Field of sender	M-0	Manufacturer identification of the M-Bus device (=sender)
	M-1	
A-Field of sender	A-0	A-field of the M-Bus device (=sender)
	A-1	
	A-2	

Field	Hex	Remark
	A-3	
	A-4	
	A-5	
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
CI	7Ah	Transport layer with short header
Access Nr	ACC-0	Access Counter (of M-Bus device)
Status	ST-0	Not used
Configuration Word	CW-0	Encryption information
	CW-1	
Encrypted Variable Data Blocks (Records) (ref section 6.4)		
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
Postamble of physical layer		

Remarks

- This message may be helpful validating the performed action after a command.

4.4.6 Unencrypted message

Specific control information, in specific circumstances, may be transmitted with an unencrypted message type. For wireless, the E-meter sends this control and configuration information to the specific M-Bus device with same SND_UD message as for the encrypted control message (see 4.4.3) and with the configuration word all zero (CW=00 00h). The acknowledgement of the M-Bus device is also the same.

4.4.7 Installation message

The M-Bus device that is put in installation mode (manually or by other means) will transmit periodically installation requests: SND_IR. This message shall contain the Short ID, and may contain as an addition data.

Field	Hex	Remark
Preamble of physical layer		
L-field	L-0	Length xx Bytes
C-Field	46h	SND_IR
MAN-Field of sender	M-0	Manufacturer identification of the M-Bus device (=sender)
	M-1	
A-Field of sender	A-0	Short ID of the M-Bus device (=sender)
	A-1	
	A-2	
	A-3	
	A-4	
	A-5	
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
CI	7Ah	Transport layer with short header
Access Nr	ACC-0	Access Counter (of M-Bus device)
Status	ST-0	Not used
Configuration Word	CW-0	Limited Access bits set. Encryption information: if no (random) User key is available, CW-1 = A0h, otherwise Method Code 15 shall be selected
	CW-1	
Variable Data Blocks (Records) (ref section 6.4) optional		
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
Postamble of physical layer		

The E-meter confirms the installation using CNF_IR:

Field	Hex	Remark
Preamble of physical layer		
L-field	L-0	Length xx Bytes
C-Field	06h	CNF_IR
MAN-Field of sender	M-0	Manufacturer identification of the E-meter (or 00 00h) (this will be ignored by the M-Bus device)
	M-1	
A-Field of sender	A-0	Short ID (or 00 00 00 00 00h) of the E-meter (this will be ignored by the M-Bus device)
	A-1	
	A-2	
	A-3	
	A-4	
	A-5	
Checksum	CS-0	2 bytes checksum for wireless FT3 format
	CS-1	
CI	80h	Transport layer without application data

Field		Hex	Remark
Short ID of M-Bus device	Identification Number	ID-0	Ident Number, e.g. 12345678 in BCD (of target M-Bus device)
		ID-1	
		ID-2	
		ID-3	
	Manufacturer ID	MAN-0	Manufacturer ID (of target M-Bus device)
		MAN-1	
	Version	VER-0	DSMR Protocol version, e.g. 42h (=4.2) (of target M-Bus device)
	Device type	DEV-0	Device type, refer to EN 13757-3 for codes (of target M-Bus device)
Access Nr		ACC-0	Access Counter (copied from of M-Bus device)
Status		00h	Not used
Configuration Word		00h	No application data, no encryption
		00h	
Checksum		CS-0	2 bytes checksum for wireless FT3 format
		CS-1	
Postamble of physical layer			

Remarks

- The exact wireless installation protocol is discussed in section 8. That section also contains information on an optional pre-configured User key for encryption.

5 ENCRYPTION LAYER

In deviation from EN 13757-3, the encryption using AES mode 15 is mandatory for all application level data during normal operation. The encryption algorithm used is AES (Federal Information Processing Standard (FIPS) 197, Advanced Encryption Standard (AES)). The following shows the encryption mechanisms and the status.

5.1 Configuration word structure

The Configuration word used in the control layer and in the encryption layer. Only the bits relevant for encryption are described here.

The configuration word is coded as follows:

MSBit 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	Bit 0
Bidirectional communicationn	Accessibility	Synchronized	Reserved	Mode bit 3	Mode bit 2	Mode bit 1	Mode bit 0	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

Mode bits 0 to 3 hold the encryption method code as outlined below.

Encryption Method Code (header configuration field)	Algorithm	Key size	Status	
			Master	Slave
x0xxh	None (no encryption)	-	M	M
xFxxh	AES128 CBC Mode 15	128	M	M

M = Mandatory

The first block of the encrypted part of any telegram will hold two filler bytes containing the value 2Fh. This is to allow verification of the decryption process

Due to the mathematical nature of the AES-algorithm the encrypted length shall be an integer multiple of 16 if the high byte signals AES-Encryption. The number of encrypted 16-byte blocks is included in the configuration word. Unused bytes in the last 16-byte block shall be filled with the filler DIF = 2Fh. To ensure message integrity at least two filler bytes should be present. In deviation from EN13757-3, at least two filler shall present. An extra data block shall be added when necessary. Both master and slave shall check the presence of these filler bytes before further processing the message.

When there is no User key available (i.e. User key is equal to zero, e.g. at installation time for wired M-Bus devices), messages are sent with encryption Method Code 0. If a User key is available (i.e. User key is not equal to zero), messages are sent with encryption Method Code 15.

5.2 Block Chaining & Frame counter

In deviation with the description in EN 13757-3, the Initialisation Vector (IV) used in Method Code 15 is in part constructed from data that is sent unencrypted as part of the message header. The IV is constructed as follows (low order bytes first):

LSB	1	2	3	4	5	6	7	8	9	10	11	12	13	14	MSB
Manuf. (LSB)	Manuf. (MSB)	ID (LSB)	..	..	ID (MSB)	Version	Medium	Frm Cnt LSB	..	..	Frm Cnt MSB	Frm Cnt LSB	..	..	Frm Cnt MSB

Frm Cnt == Frame counter as specified in the message with VIF FDh, 08h. This Frame counter is repeated twice. The data block containing the frame counter is not encrypted and inserted between the (encrypted) filler bytes and CS.

The receiver of a message, either the E-meter or the M-Bus device, shall check the validity of the frame counter.

The encrypted message is validated as follows:

1. the received frame counter must be higher than the previously validated frame counter;
2. the received message is encrypted and received correctly, i.e. checksum and other M-Bus fields are correct;
3. the message is decrypted correctly, i.e. the integrity field (two filler bytes) is present.

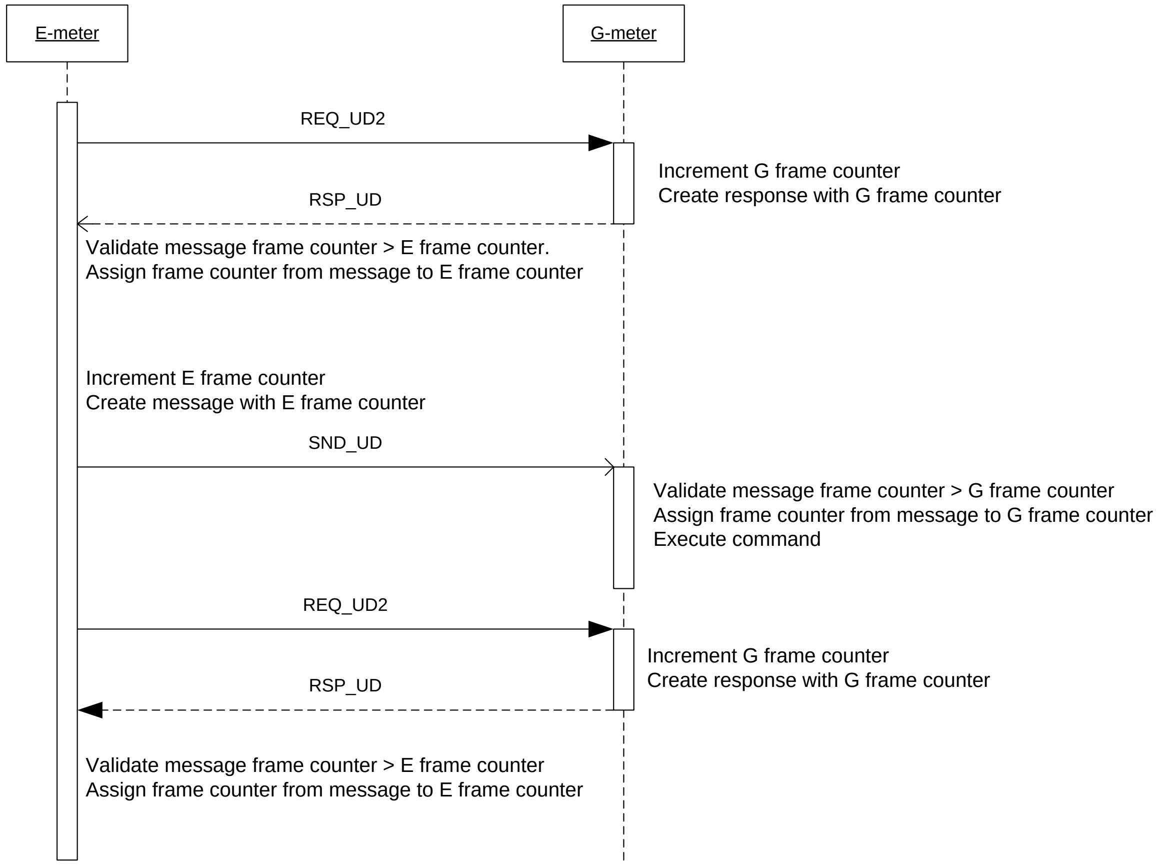
Only encrypted messages that conform to this validation rule shall be accepted by the receiving device. Unencrypted messages and messages that use encryption code 0 will not contain frame counters.

After this validation of an encrypted message, the received frame counter is stored as validated frame counter and is ready for the next usage, either sending or receiving a new message.

When the device sends a new message, the frame counter is incremented by the sender exactly 1 (one).

With all encrypted messages, the IV uses the information of the M-Bus device. So, if the M-Bus is the sender, the information for bytes 0-7 of the IV is taken from the address field (A-field) containing the M-Bus address. If the M-Bus is the receiver, the information for bytes 0-7 of the IV is derived from the Short ID of the M-Bus located in the 12 bytes Long Data Header.

Figure 4 Sequence diagram for wired M-Bus devices:


E-meter
G-meter
REQ_UD2
Increment G frame counter
Create response with G frame counter
RSP_UD
Validate message frame counter > E frame counter.
Assign frame counter from message to E frame counter
Increment E frame counter
Create message with E frame counter
SND_UD
Validate message frame counter > G frame counter
Assign frame counter from message to G frame counter
Execute command
REQ_UD2
Increment G frame counter
Create response with G frame counter
RSP_UD
Validate message frame counter > E frame counter
Assign frame counter from message to E frame counter

It is important to realize that the G-meter is the owner of the frame counter and the E-meter is merely using it:
When a message that comes from the G-meter gets lost, the E-meter will not have the latest frame counter and might send messages that are ignored by the G-meter. If the G-meter does not respond to the commands of the E-meter, the E-meter shall issue a REQ_UD2, to establish the current value of the frame counter from the G-meter. It will still compare the frame counter it received from the G-meter with the previous message so that replay is impossible.
The use of one frame counter owned by the Gas meter also facilitates easy exchange of E-meters. There is a possibility for replay attacks directly after the Gas meter is installed, but the timestamp and reading in the RSP_UD or SND_NR will make sure these are easily spotted (the E-meter is not receiving the latest reading, but a reading that was received earlier by the previous meter). This makes it important that the E-meter records the time stamp that is included in the RSP_UD or SND_NR.

The frame counter is never reset during the life time of the G-meter.

Note : An efficient “wireless” implementation of this protocol in the E-meter would probably predict the frame counter and encrypt the messages to be sent to the M-Bus device before the hourly message from the M-Bus device is actually received. Synchronizing the time might require a more complex approach.

5.2.1 Example Initialization Vector

Example 1 shows an Initialization Vector as it might be sent to and from a M-Bus device.

Field	Hex	Remark
Manufacturer ID	B4h	Manufacturer ID ‘NET’
	38h	
Identification ID	89h	Identification Number, e.g. 23456789
	67h	
	45h	
	23h	
Version	42h	DSMR Protocol version
Medium	03h	Medium, e.g. gas
Frame counter	01h	Frame Counter of the current telegram
	00h	
	00h	
	00h	
Frame counter	01h	
	00h	
	00h	
	00h	

Example 1: Initialization Vector

6 APPLICATION LAYER

This part of the document describes the required M-Bus communication protocol between the residential electricity meter, functioning as M-Bus master, and M-Bus slave devices.

The installation part, such as the installation process of an external M-Bus device, removing an external M-Bus device, exchanging an external M-Bus device, is described for both wired and wireless devices in section 8.
The application layer includes the data that is transmitted. For the M-Bus protocol the data structures and data types of the application layer are described in EN 13757-3.
Filler bytes (DIF=2Fh) may be used in unencrypted variable datablocks and must be used in encrypted variable datablocks.

Application layer message structures are the same for wired and wireless systems.

6.1 Meter Value Transfer

M-Bus devices can transfer either actual values or hourly values. If a clock is present then the hourly values are stored by the M-Bus device every whole hour. One hourly value including M-Bus device time stamp is stored.
The M-Bus transfer will use the Storage Number bit in the DIF block to signify the hourly value.

6.2 Commands

6.2.1 Set Date and Time Procedure

If the M-Bus device has an internal clock it should be synchronised by the master system. Synchronisation is done:

- At every time change of the Bus Master
- Every day to ensure a maximum deviation below 60 seconds.

The maximum allowed clock deviation between E-meter and M-Bus device is 60 seconds. If the M-Bus device receives a new system time through the Set Date and Time mechanism then it verifies the difference between the new time and the old M-Bus Device system time. If the difference is more than 60 seconds then a “Clock synchronization error” is set (ref 6.3.3). The M-Bus device will always set its system time to the time received in the synchronisation message. The time used in the P2 messages is UTC. Format Type I specified in prEN 13757-3 is intended for local time but in this companion standard it shall be used for UTC[4]

[4] The fields ”Second”, “Minute”, “Hour”, “Day”, “Month”, “Year”, “Day of Week”, “Week”, “Leap year” shall contain the UTC time. The fields “Time during daylight saving” and “Daylight saving deviation” shall not be used and coded as “0”. Example: UTC time 16 July 2013; 13:00 shall be coded as ”Second=0”, “Minute=0”, “Hour=13”, “Day=16”, “Month=7”, “Year=13”, “Day of Week=2”, “Week=0”, “Leap year=0”, “Time during daylight saving=0” and “Daylight saving deviation=0”. M-Bus devices shall ignore the fields “Time during daylight saving” and “Daylight saving deviation”.

The time is set using the following message with the special CI-code:

Field	Hex	Remark
	2Fh, 2Fh	Filler bytes
TC	00h	Set time
	xxh, xxh, xxh, xxh, xxh, xxh	New time in Format I (but used for UTC; see remark)
	00h,00h,00h	Reserved
	2Fh, 2Fh, 2Fh, 2Fh	Filler bytes

When the User key is set (non zero value), this command can only be send encrypted. If the User key is not set, this command can be send unencrypted.

6.2.2 Set new address

To change the primary address (wired meters only) from zero to an open address the E-meter (Master) has to write address data to the M-Bus device.

Field	Hex	Remark
DIF	01H	Data identifier
VIF	7AH	Address data
A	xxH	Address field new

Notice that this telegram is always sent unencrypted. To prevent Denial of Service attacks that makes the M-Bus device inaccessible (setting the M-Bus device at any M-Bus address); the M-Bus device shall conditionally accept this telegram.

Note : M-Bus devices shall only accept this telegram when the User key is not set (equivalent to the User key set to zero). M-Bus devices shall ignore this telegram when the User key is set unequal to zero to prevent fraud by setting the M-Bus device to an unreachable M-Bus address.
To set the M-Bus device to another M-Bus address, the AMI system needs to set the User key to zero first. Then the Master may set the M-Bus device to a new address.

6.2.3 Clearing the Status byte

The Status byte has the following meaning:

Bit	Meaning with Bit set	Significance with Bit not set
0,1	Application errors, see EN 13757-3	Application errors, see EN 13757-3
2	Power low (Battery replacement expected)	Not power low
3	Permanent error	No permanent error
4	Temporary error	No temporary error
5	Clock Synchronisation error: more than 60 seconds deviation	No significant clock deviation.

6	Fraud attempt registered	No fraud attempt registered
7	Reserved for backwards compatibility - value = 0	Reserved for backwards compatibility – value = 0

There is a distinction between permanent errors (battery error and permanent error) and non-permanent errors (all other errors).

The E-meter should clean the status byte after each time a non-permanent error is retrieved from the M-Bus device by sending:

Field	Hex	Remark
DIF	01h	8 bits
VIF	FDh	Use a VIFE
VIFE	97h	Error Flags
	06h	Clear the bits
Mask	73h	01110011

Details can be found in EN 13757-3 chapter 9.

6.2.4 Set new key

See 6.5.1.

6.3 Readout List

The read out list specifies which data blocks are sent by default.

Meter specific data blocks are defined in section 6.4. The order in which data blocks are inserted in an RSP-UD (wired and wireless) or SND_NR (wireless only) frame is not specified. The following holds:

- Data Information Fields (DIF) and Value Information Fields (VIF) are mandatory and are coded as in EN 13757-3.
- Extended Data Information Fields (DIFE) and Extended Value Information Fields (VIFE) are mandatory to distinguish tariff based values or special units.

All types slave meter will send the following data if not specifically polled for a specific data item:

- 4.3.2 and 0 Data Header
- 6.3.3 Status byte
- 6.4.1 Equipment Identifier
- 6.4.8 Meter Configuration Data

All M-Bus devices transfer the last known hourly value (Storage Number bit in DIF field is set) and a time stamp indicating the time of the meter reading value.

- 6.4.3 Time stamp
- 6.4.3 Gas Meter specific data blocks:
  - Converted volume (6.4.4)

Thermal meters (device type =x0D) will send the following data items if not polled for a specific data item:

- 6.4.5 Thermal (heat / cold) Meter specific data blocks:
  - Hourly meter reading heat if this is in the meter configuration data

- Hourly meter reading cold if this is in the meter configuration data
- Hourly meter reading volume if this is in the meter configuration data

Water meters (device type = x07) will send the following data items if not specifically polled for a specific data item:

- 6.4.6 Water Meter specific data blocks: Hourly meter reading volume.

6.3.1 Changing the readout list

The readout list can be changed with a SND_UD and data records containing the data field 1000b, which means “selection for readout request”. The following VIF defines the selected data as listed in EN 13757-3 and no data are transmitted. The answer data field is determined by the slave. The master can select several variables by sending more data blocks with this data field in the same telegram.

The actual values can be retrieved by subsequently issuing a REQ_UD2. The master should restore the default readout list immediately after it retrieved the data. This shall be supported by the M-Bus device only.

When changing the readout list does not succeed the first time, a maximum of 2 retries should be performed.

6.3.2 Resetting the readout list

The readout list can be reset by sending a SND_NKE. For wireless, the readout list is also reset by terminating the FAC (either by time-out or command; the FAC is also terminated by sending SND_NKE).

6.3.3 Reading the Status byte

The Status byte has the following meaning:

Bit	Meaning with Bit set	Significance with Bit not set
0,1	Application errors, see EN 13757-3	Application errors, see EN 13757-3
2	Power low (Battery replacement expected)	Not power low
3	Permanent error	No permanent error
4	Temporary error	No temporary error
5	Clock Synchronisation error: more than 60 seconds deviation	No significant clock deviation.
6	Fraud attempt registered	No fraud attempt registered
7	Reserved for backwards compatibility - value = 0	Reserved for backwards compatibility - value = 0

There is a distinction between permanent errors (battery error and permanent error) and non-permanent errors (all other errors).

The E-meter can retrieve the status from the M-Bus device from the M-Bus device by sending:

Field	Hex	Remark
DIF	01h	8 bits
VIF	FDh	Use a VIFE
VIFE	17h	Error Flags

6.4 Variable Data Blocks

Note that all variable data blocks must be send encrypted when the User key is set (equivalent to the User key set to a non-zero value).

Variabele data blocks containing measurement data shall be handled by the E-meter (even when unencrypted) to be able to provide data for the P1 port.

6.4.1 Equipment Identifier

Field	Hex	Remark
DIF	0Dh	Variable length ASCII
VIF	78h	Equipment identifier
LVAR	11h	Length 17
	34h, 33h, 32h, 31h	Equipment identifier 17 ASCII, e.g. ABCD1234567891234
	39h, 38h, 37h	
	36h, 35h, 34h	
	33h, 32h, 31h	
	44h, 43h, 42h, 41h	

All meters are uniquely identified by a 17 ASCII character Equipment identifier.

Note : If the meter code is shorter than 5 characters, leading spaces (coded as 20h) shall be added.

Note : If the serial number is shorter than 10 characters, leading zeroes (coded as 30h) shall be added.

6.4.2 Remote read of firmware and hardware versions

The P2 interface must support remote reading of firmware and hardware versions. Using the following VIF's (DIF = 08h):

VIF/VIFE = FDh 0Ch ("Model / Version"),
VIF/VIFE = FDh 0Dh ("Hardware version number") for the Hardware version,
VIF/VIFE = FDh 0Eh ("Metrology (firmware) version number"),
VIF/VIFE = FDh 0Fh ("Other firmware version number") for the firmware version.

These VIF/VIFE's should not be added to the readout list by default. The master can add and remove these VIF/VIFE by issuing a 'selection for readout request'.

To identify the various HW, FW and configuration versions, the M-Bus device shall use properties in the response string. A property is defined as "*name=value*".

The following properties are mandatory.

Type	VIFE			
	0Ch	0Dh	0Eh	0Fh
DSMR Protocol	dsmr=			
Metrology FW			met=	
Metrology HW		met=		
Communication FW				com=
Communication HW		com=		
Application FW				apl=
Application config				cfg=

Application configuration is used to identify a set of parameter values that determines the behaviour of the meter. These parameters are set during production of the meter.

Each property is to be terminated with CR/LF (ASCII characters <CR><LF>), also when multiple properties are combined in a single response.

Examples (actual text usage free to supplier):

VIF/VIFE = FDh 0Dh
Return value:
met=PCBx1.x2<CR><LF>
com=M-Bus module supplier<CR><LF>

VIF/VIFE = FDh 0Eh
Return value:
met=FW123.4.5<CR><LF>

6.4.3 Time stamp

M-Bus devices transfer either actual values or hourly values, either value will be accompanied with a time stamp of the moment the value is determined. The Storage Number bit in the DIF block of the time stamp signifies the hourly value. The time stamp is UTC and sent in Format I.

Field	Hex	Remark
DIF	46h	6 bytes integer, storage bit set
VIF	6Dh	Extended Date and Time compound data type I
	xxh, xxh, xxh, xxh, xxh, xxh	Date/Time (yy.mm.dd.hh:mm:ss)

6.4.4 Gas Meter specific data blocks

Gas Meter specific data blocks contain the Meter Reading temperature converted Volume. The storage bit should be set for hourly values. For Gas Meters G10-G25 the display is in 10 Litre resolution, therefore separate VIFs are necessary.

For G4-G6:

Field	Hex	Remark
DIF	4Ch	8 digit BCD (storage bit is set for hourly values)
VIF	13h	Multiplier 0,001; unit m^3
	43h	Temperature converted reading, e.g. 31412,743 m^3
	27h	
	41h	
	31h	

For G10-G25:

Field	Hex	Remark
DIF	4Ch	8 digit BCD (storage bit is set for hourly values)
VIF	14h	Multiplier 0,01; unit m^3
	43h	Temperature converted reading, e.g. 314127,43 m^3
	27h	
	41h	
	31h	

6.4.5 Thermal (heat / cold) Meter specific data blocks

To differentiate between Heat and Cooling values the Device Unit in the DIFE field is used. For Cooling values the Device bit is set to TRUE. For Heat values the DIFE field is omitted or the Device bit in the DIFE is set to FALSE.

Meter Reading Energy Heat

Field	Hex	Remark
DIF	4Ch	8 digit BCD (storage bit is set for hourly values)
VIF	0Fh	Multiplier 0,01 ; unit GJ
	27h	Meter reading, e.g. 03141,27 GJ
	41h	
	31h	
	00h	

Meter Reading Energy Cold

Field	Hex	Remark
DIF	CCh	8 digit BCD (storage bit is set for hourly values)

DIFE	40h	Cooling unit
VIF	0Fh	Multiplier 0,01 ; unit GJ
	27h	Meter reading, e.g. 03141,27 GJ
	41h	
	31h	
	00h	

Meter Reading Volume

Field	Hex	Remark
DIF	4Ch	8 digit BCD (storage bit is set for hourly values)
VIF	13h	Multiplier 0,001; unit m^3
	74h	Meter reading, e.g. 02440,474m^3
	04h	
	44h	
	02h	

6.4.6 Water Meter specific data blocks

Meter Reading Volume

Field	Hex	Remark
DIF	4Ch	8 digit BCD (storage bit is set for hourly values)
VIF	13h	Multiplier 0,001; unit m^3
	74h	Meter reading, e.g. 03141,274 m^3
	12h	
	14h	
	03h	

6.4.7 Slave E meter specific data blocks

Meter Reading (“

Field	Hex	Remark
DIF	4Ch	8 digit BCD (storage bit is set for hourly values)
VIF	03h	Multiplier 1; unit Wh
	74h	Meter reading, e.g. 03141274 Wh
	12h	
	14h	
	03h	

6.4.8 Meter Configuration Data

This data item holds a single block showing which measurements are implemented. Note that the meter type is defined in the data header (ref Device Type in 4.3.2 and 0)

Field	Hex	Remark
DIF	01h	1 digit binary

VIF	FDh	Extension
VIFE	67h	Note this was marked as “Special Supplier Information” in EN 13757-3
Mask	XXh	See below

The table below specifies the meaning of each bit (0 = false, 1 = true) in the mask attribute.

Bit	Meaning
0	Clock device implemented
1	Valve device implemented
2	Meter type Gas only: Converted volume This bit is set when the temperature converted value is indicated on the display and transmitted via M-Bus.
3	Valve release command is supported
4	Valve open direct command is supported

6.5 Key Management Procedures

Every M-Bus device is configured by the supplier with a Default key. The supplier guarantees that every meter has a unique key. This Default Key is registered with the device’s Equipment Identifier (ref 6.4.1) or Short ID (ref 4.2.2). The value of the Default key cannot be deducted from any combination of the values of the attributes of the M-Bus device (the key is chosen randomly). This Default key is used exclusively to decrypt every new User key that is received over the M-Bus. The Default key will never be renewed.

The User key is used to encrypt all messages. The User key is transferred to the Electricity meter over P3 and the same key is, encrypted with the M-Bus devices Default key, transferred to the Electricity meter and from there it is transferred to the M-Bus device. The M-Bus device will decrypt this new User key using its Default key and from then on will use the newly received User key.

- Initially, the wired M-Bus has no User key and all messages are sent unencrypted, until a new User key is received and decoded.

Once the User key is set unequal to zero, the M-Bus master will only accept encrypted data and the M-Bus will only accept encrypted commands, with exception of the following that will be accepted unencrypted:

- Set new key (using CI=51h/5Bh, DIF=07h, VIF=FDh, VIFE=19h, DIF=47h, VIF=FDh, VIFE=19h)
- Data Request REQ_UD2

Note that the command for setting a new M-Bus address is not accepted unencrypted once the M-Bus device has set the User key unequal to zero.

Note that key changes can occur at any time during the operation of the M-Bus devices. Note that with ALL key changes the M-Bus device receives the new key encrypted with the device's default encryption key.

6.5.1 User key exchange procedures

After installation the M-Bus device is queried for (wired devices) or sends (wireless devices) meter reading data. These transmissions contain the unencrypted Short ID.
The electricity meter will make this Equipment identifier available to the CS.
Typically, the CS will transfer a new key for the M-Bus device through the (encrypted) P3 channel to the Electricity meter. M-Bus Client Setup objects (0-x:24.1.0.255) handle User keys of M-Bus devices. Method 8 - transfer_key is used for this purpose. Its purpose is to transfer the User key into the M-Bus device. The User key is transferred encrypted with the Default key and the CS performs this encryption.

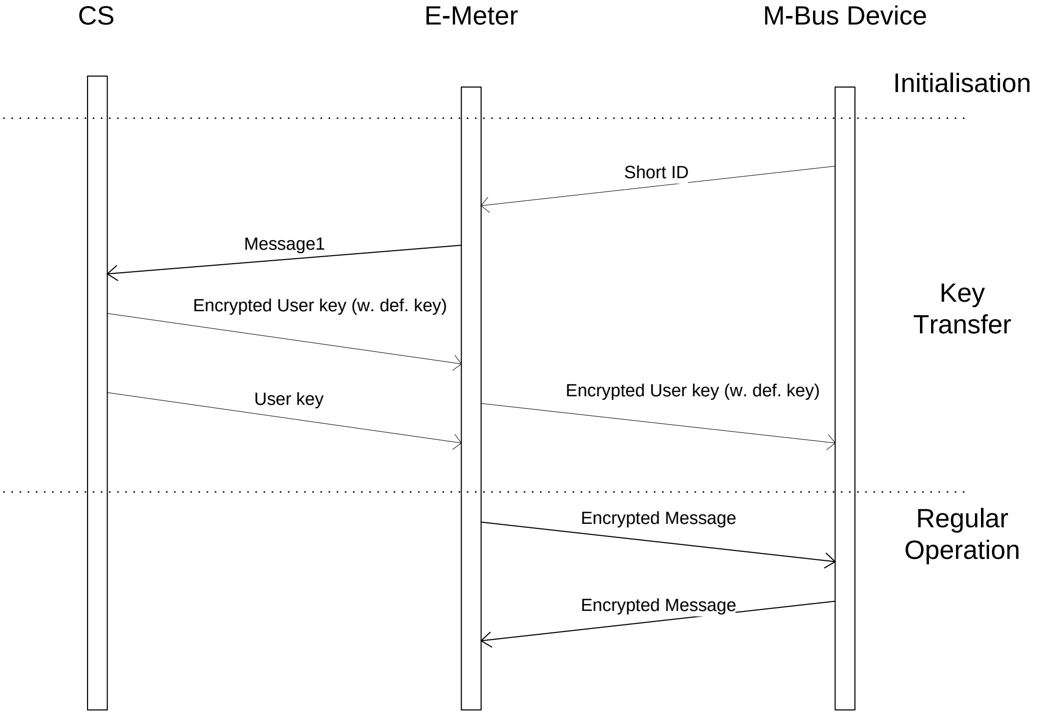


Figure 5: Key exchange procedure

This new key is transferred through P3 as plain octet string, for use in the electricity meter, and as octet string encrypted by the M-Bus device's Default key.
The encrypted string is transferred over the P2 interface, using an unencrypted message type. This is a deviation from DLMS BlueBook version 10.The M-Bus device receives the encrypted string as a series of 64 bit integers, least significant byte first, VIF= FDh, VIFE=19h (formerly reserved VIFE). The second 64 bit string will have the storage bit in the DIF set.

Field	Hex	Remark
DIF	07h	64 bit data, Storage 0 => (64 LSB bits of encryption key)
VIF	FDh	VIF from table 11

VIFE	19h	Reserved -> AES 128 KEY exchange
AES KEY1	19h	AES KEY 1->8, where AES KEY1 is the LSB in the LSB half of the key.
AES KEY2	1Eh	
AES KEY3	12h	
AES KEY4	D8h	
AES KEY5	0Ch	
AES KEY6	00h	
AES KEY7	F6h	
AES KEY8	70h	
DIF	47h	64 bit data, Storage 1 => (64 MSB bits of encryption key)
VIF	FDh	VIF from table 11
VIFE	19h	Reserved -> AES 128 KEY exchange
AES KEY9	32h	AES KEY 9->16, where AES KEY9 is the LSB in the MSB half of the key.
AES KEY10	99h	
AES KEY11	85h	
AES KEY12	71h	
AES KEY13	39h	
AES KEY14	22h	
AES KEY15	48h	
AES KEY16	69h	

The M-Bus device will concatenate the 64 bit integers, and decrypt the octet string using its Default key and will use the resulting 128 bit key in encryption / decryption of further communications.

Setting the User Key to “00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h” means no User Key is defined, i.e. all subsequent communication is unencrypted.

The User Key is encrypted with the Default Key, using AES-128

6.5.2 Key Management Requirements

Both the Default Encryption Key and the currently in use User key are to be registered in the back office. Both keys are expected to be unique for every individual meter.

All wired M-Bus devices are delivered with Default key but without User key (no key set). Otherwise the M-Bus address cannot be changed from address 0. All wireless M-Bus device may be delivered with or without User key, as will be indicated as a configuration option. If the User key is set, it is used by the M-Bus device for initial transmissions (SND_IR) and all other transmissions involving meter reading data. If the User key is not set by the vendor, these transmissions are sent unencrypted. Notice that the User key may not be available in the E-meter. However, the unencrypted headers of the M-Bus transmissions contain sufficient information (Short ID) for the initial installation process.

7 POWER SUPPLY

7.1 Maximum current

The bus interface - that is, the wired interface between the slave and the bus system – can take the power it requires from the bus system. The interface of the slave shall be fed from the bus. The M-Bus standard defines M-Bus loads of up to 1,5 mA whereby any external device can use up to 4 M-Bus unit loads. The M-Bus master shall be capable of supplying at least 16 M-Bus unit loads (4 devices of up to 4 M-Bus loads each). Note also the physical layer specifications in EN 13757-2 section 4.

Wireless devices have their own power source.

7.2 Power outage

A power outage on the M-Bus wired connection could occur. M-Bus devices should always measure and register the usage during a power outage. All configuration data (including M-Bus device addresses and User keys) and all process data are to be stored during long power outages. Wireless devices need not necessarily detect power failures of the electricity meter and the connected communication device. The meter reading that is registered, the meter reading that is sent to the electricity meter and the meter reading on the meter's display should be consistent at all times. Any registered interval data may be lost during power outage.

8 INSTALLATION PROCEDURES

The flowchart for entering the different modes in the gasmeter is described in Appendix C.

8.1 General installation procedures

During installation the M-Bus devices will be registered by the E-meter.

Removal of the M-Bus cover at the E-meter or a power-up of the E-meter are possible triggers to set the E-meter in Installation mode.
When in installation mode the E-meter:

- the E-meter scans for physically connected wired M-Bus devices and accepts and processes installation mode requests (SND_IR) from wireless M-Bus devices.
- at least the last 7 digits of the meter number (equipment identifier) of all wireless M-Bus devices found will be shown on the display of the E-meter.
- If a new device is detected it must be added to the list of detected device ID's
- By pressing the button at least 2 seconds a selection is made and the binding process is started.

When the M-Bus cover at the E-meter is replaced, the E-meter exits Installation mode.

After the M-Bus devices are registered in the E-meter and M-Bus devices are in Customer mode, several administrative tasks shall be executed. The User keys need to be transferred before the readout list is changed. The readout list is changed to read out the firmware and hardware versions and the meter configuration data during the installation procedure. The standard readout list is activated by sending a SND_NKE.

For identification of the M-Bus devices in the E-meter as well as in the back office, the Short ID shall be used. The back office maps the Short ID to other identifiers like the Equipment Identifier, if needed.

8.2 M-Bus Device State

M-Bus devices can be in one of four states:

- Storage mode: the wireless M-Bus interface is inactive.
- Installation mode: In installation mode, wired M-Bus devices accept settings from the E-meter; wireless M-Bus devices will broadcast requests so that an E-meter can register it.
- Customer mode: after a wired M-Bus device receives an M-Bus address and after a wireless M-Bus device receives its CNF_IR, it will start normal operation in Customer mode as described elsewhere in this document.
- Test mode: a vendor specific mode; not in the scope of this document.

8.3 Wired configurations

8.3.1 Scan for new M-Bus devices

The E-Meter will maintain a list of device addresses, in the range 1 to 250, of all devices it is connected to, through a wired connection. Note that only four M-Bus devices can be connected, either wired or wireless. While in installation mode, the E-meter will continuously scan for devices on the wired M-Bus. All responding devices will be registered in the list. This scan will be suspended for any other data transfer. The scan and the installation mode will be terminated if four devices are registered, after the M-Bus cover is replaced or 1 hour after the scan was triggered by a power-up of the E-meter or removal of the M-bus cover. The E-meter will support two types of addresses to discover newly installed M-Bus devices:

- Devices with address 0
  Address 0 is reserved for unconfigured M-Bus devices. Each unconfigured M-Bus device shall accept and answer all communication to this address (ref EN 13757-2 section 5.7.5 and this companion standard section 4.3.1).
  The E-meter will select an unused device address and set the new M-Bus device's address to that using the procedure in 6.3.2.

- Devices with unregistered address
  The E-meter will scan all unused addresses once per minute following the procedure outlined in EN 13757-3 section 11.5. Note that there is only one baud rate allowed and that secondary addresses are not used.

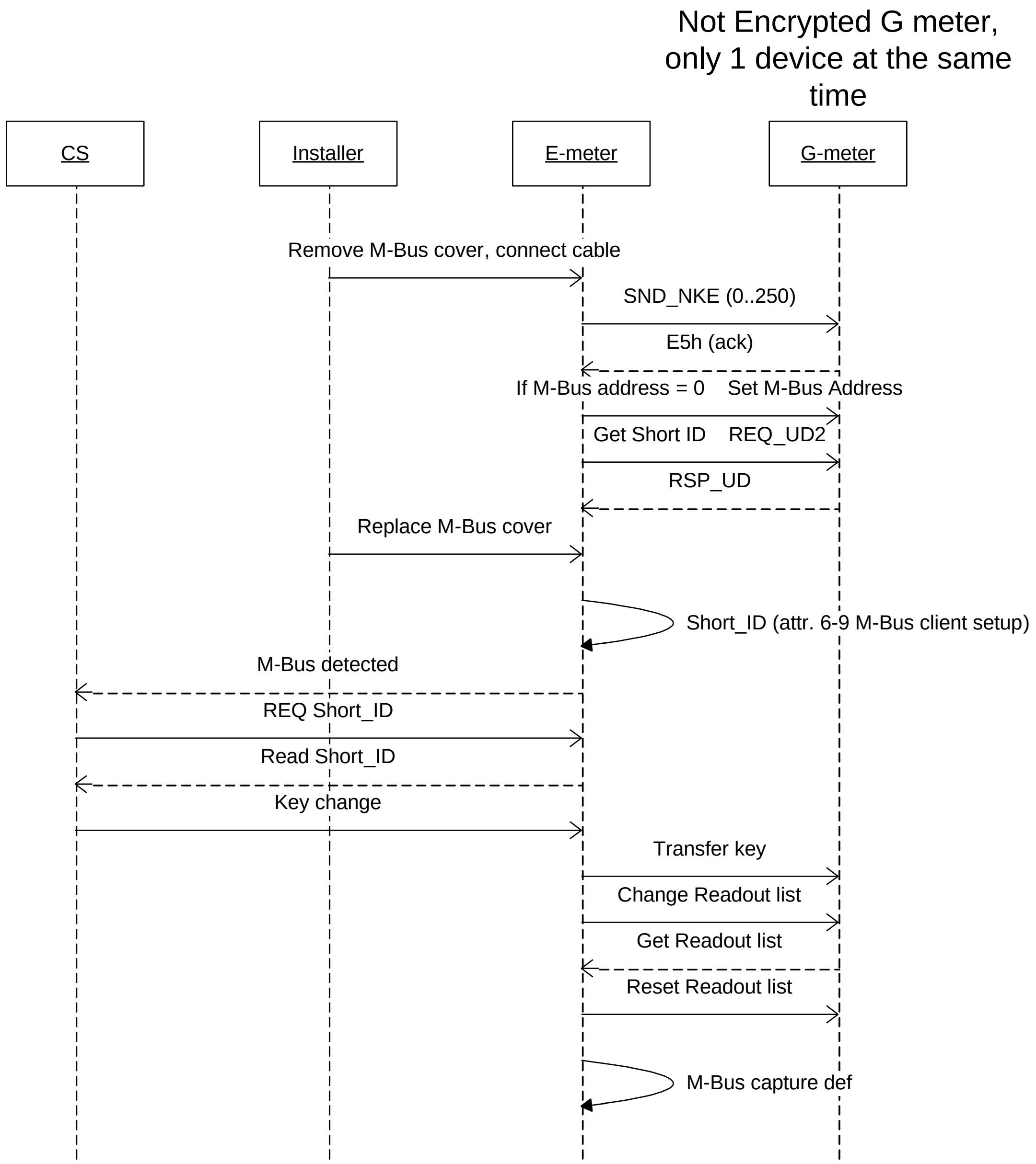


Figure 6: Example wired installation with unencrypted gasmeter.

Figure 6 describes how an installer manually starts the M-bus installation process by removing the M-bus cover on the E-meter to start the installation mode on the E-meter. The gasmeter is delivered without an User-key. In this example actions like time-synchronisation and exchange of unencrypted data is not included.

8.3.1.1 Remote wired M-Bus binding via CS by writing attributes of the M-Bus Client Set-up Object

This scenario handles the process of binding a preconfigured wired G-meter (in general a M-Bus device) to an E-meter which is not bound yet to this M-Bus device and has not automatically scanned (or not successfully scanned) for these M-Bus devices.

Trigger	Description
Exchange Measuring equipment	During installation of the Measuring equipment, the normal (wired) M-Bus scan process is not executed, e.g. power off during installation and “discover_on_power_on” is disabled. The wired M-Bus device has already a non-zero primary address, for instance from a previous installation. This situation may occur for an existing installation where the E-meter is replaced, or where a preconfigured G-meter is installed.
Corrective action by Operations	For refreshing settings in the CS or Measuring equipment, Operations remotely de-installs and reinstalls the M-Bus device.

Figure 7 shows the scenario in high-level steps. Either the E-meter or the G-meter is placed or exchanged and the local binding was, purposely or accidentally, not executed.

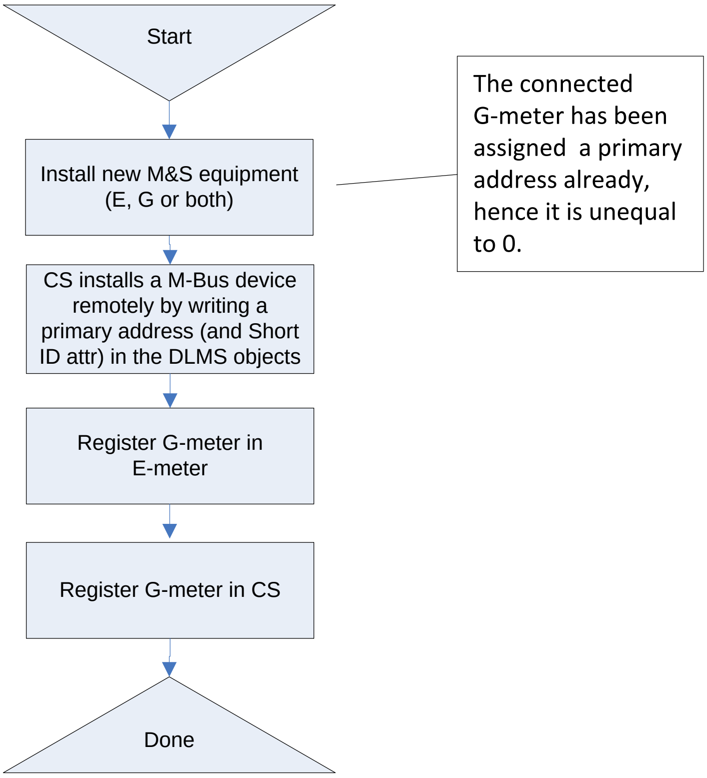

Start
Install new M&S equipment (E, G or both)
CS installs a M-Bus device remotely by writing a primary address (and Short ID attr) in the DLMS objects
Register G-meter in E-meter
Register G-meter in CS
Done
The connected G-meter has been assigned a primary address already, hence it is unequal to 0.

Figure 7: Wired: Configuring DLMS M-Bus attributes in E-meter

Pre-conditions

- The E-meter is not bound to the physically connected M-Bus device;
- The M-Bus device is preconfigured with a non-zero primary address.

Parameters

- DLMS M-Bus Client Setup (Class ID: 72) in the E-meter, specifically primary_address and Short ID attributes;
- Primary address of M-Bus device itself, already assigned and known in the CS.

Post-conditions

- Binding of E-meter and wired M-Bus device;
- Logging of the event ‘M-Bus device detected’.

Assumptions

- After transferring the keys by the CS, the E-meter shall autonomically set the capture definition, change and get the read-out list and set the clock.

Reference

- DLMS Blue Book
  This scenario is an implementation (of which variations are possible, see also text in the figure) of the requirement for attribute 5, primary_address, at section 4.7.2.

The sequence diagram is shown in Figure 8:

Scenario 2.1: Binding of wired M-Bus with M-Bus attributes

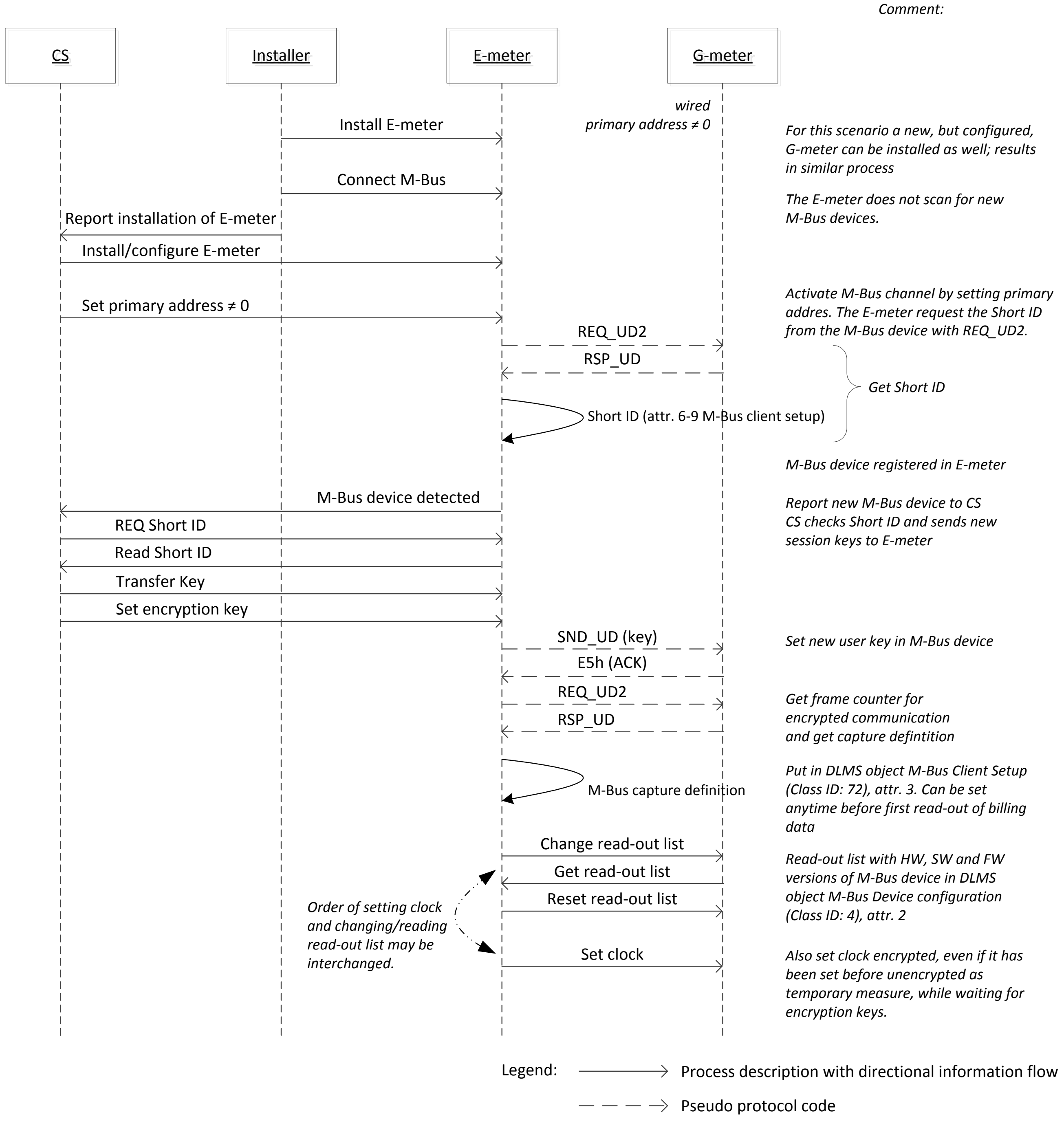

Comment:
CS
Installer
E-meter
G-meter
wired
primary address ≠ 0
Install E-meter
Connect M-Bus
Report installation of E-meter
Install/configure E-meter
Set primary address ≠ 0
REQ_UD2
RSP_UD
Short ID (attr. 6-9 M-Bus client setup)
M-Bus device detected
REQ Short ID
Read Short ID
Transfer Key
Set encryption key
SND_UD (key)
E5h (ACK)
REQ_UD2
RSP_UD
M-Bus capture definition
Change read-out list
Get read-out list
Reset read-out list
Set clock
Order of setting clock and changing/reading read-out list may be interchanged.
For this scenario a new, but configured, G-meter can be installed as well; results in similar process
The E-meter does not scan for new M-Bus devices.
Activate M-Bus channel by setting primary addres. The E-meter request the Short ID from the M-Bus device with REQ_UD2.
Get Short ID
M-Bus device registered in E-meter
Report new M-Bus device to CS
CS checks Short ID and sends new session keys to E-meter
Set new user key in M-Bus device
Get frame counter for encrypted communication and get capture defintition
Put in DLMS object M-Bus Client Setup (Class ID: 72), attr. 3. Can be set anytime before first read-out of billing data
Read-out list with HW, SW and FW versions of M-Bus device in DLMS object M-Bus Device configuration (Class ID: 4), attr. 2
Also set clock encrypted, even if it has been set before unencrypted as temporary measure, while waiting for encryption keys.
Legend:
Process description with directional information flow
Pseudo protocol code

Figure 8: Sequence diagram of binding a wired M-Bus device with M-Bus attributes.

8.3.1.2 Remote wired M-Bus binding via CS by using the slave_install() method

This scenario handles the process of binding a wired G-meter (in general a M-Bus device) to an E-meter which is not bound yet to this M-Bus device and has not automatically (or successfully) scanned for these M-Bus devices.

Trigger	Description
Exchange Measuring equipment	During installation of the Measuring equipment, the normal (wired) M-Bus scan process is not executed, e.g. powered E-meter has “discover_on_open_cover” disabled. This is a typical situation when an installation process via the CS is configured.
Corrective action by Operations	For refreshing settings in the CS or Measuring equipment, Operations remotely de-installs and reinstalls the M-Bus device.

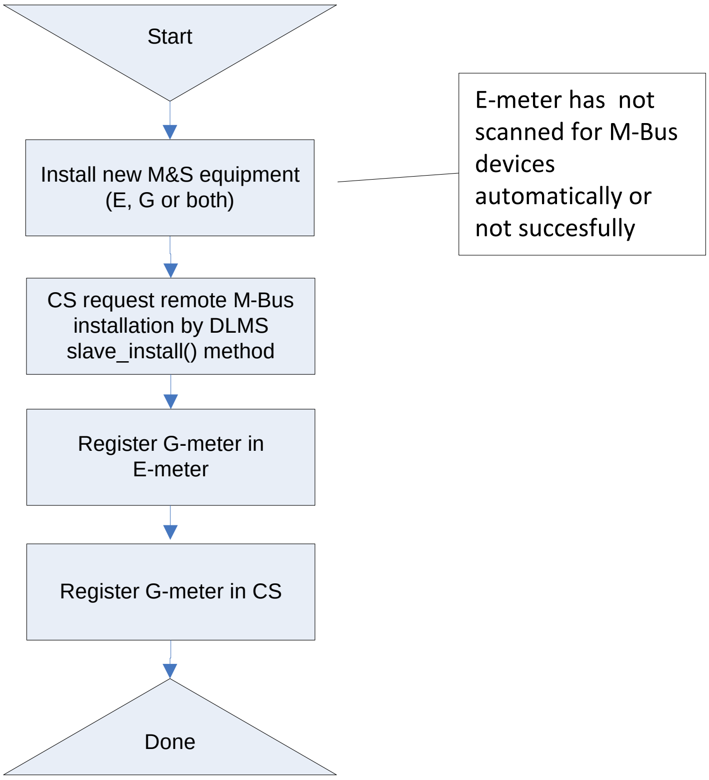

Start
Install new M&S equipment (E, G or both)
E-meter has not scanned for M-Bus devices automatically or not succesfully
CS request remote M-Bus installation by DLMS slave_install() method
Register G-meter in E-meter
Register G-meter in CS
Done

Figure 9: Wired: Configuring DLMS M-Bus attributes in E-meter

Figure 9 shows the scenario in high-level steps. Either the E-meter or the G-meter is placed or exchanged and the local binding was, purposely or accidentally, not executed.

Pre-conditions

- The E-meter is not bound to the physically connected M-Bus device;

- The M-Bus device is in one of the following states:
    - Unconfigured (primary address is 0) and unencrypted;
    - Preconfigured with a non-zero primary address and either encrypted or unencrypted.

Parameters

- *None*

Post-conditions

- Binding of E-meter and wired M-Bus device.

Assumptions

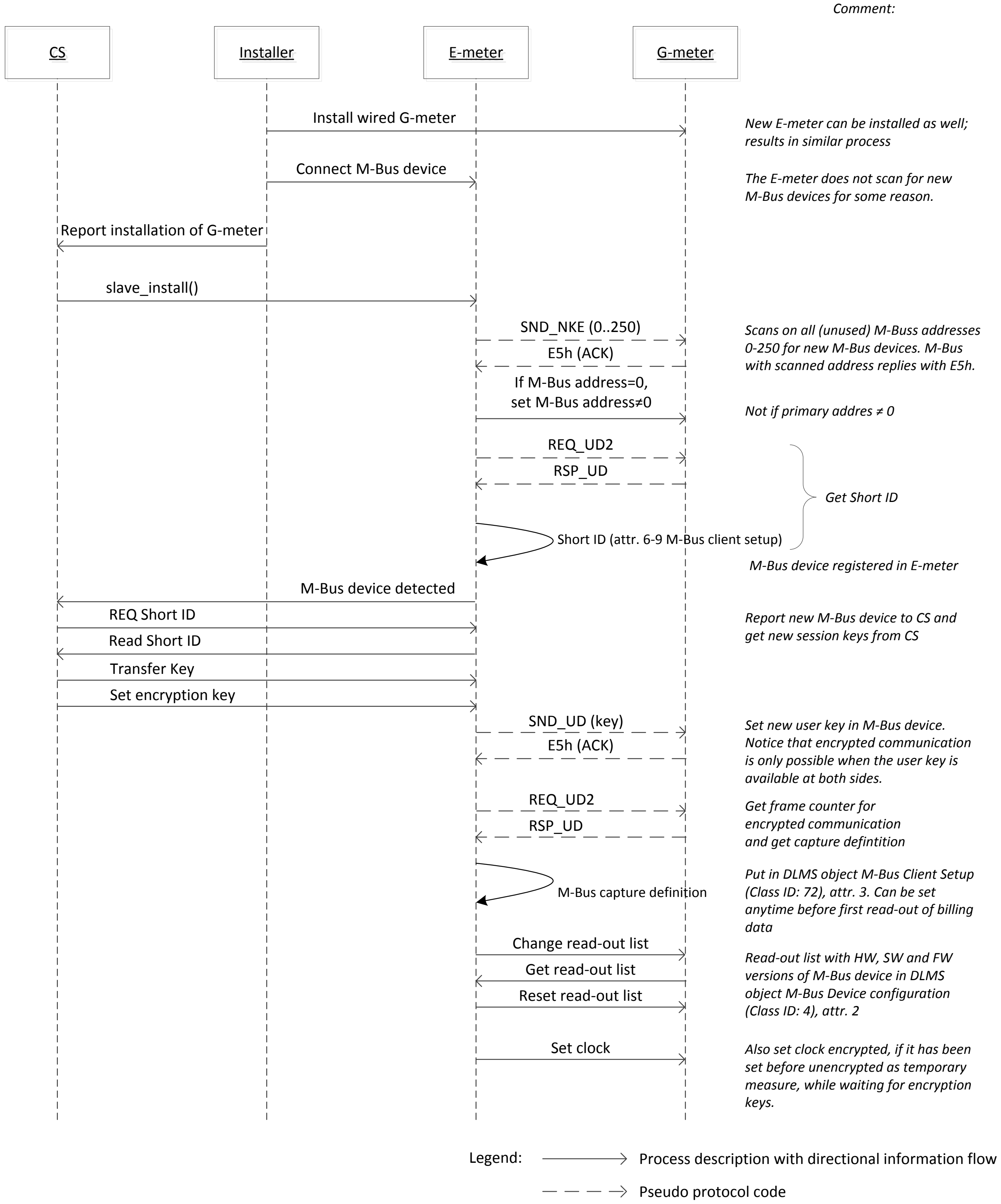
- The DLMS slave_install() method in the DLMS specification is adapted to scan on both primary address 0 as well as 1-250 (when not already in use).
- Triggered by the slave_install(), the regular installation procedures shall be performed (change M-Bus address if needed, set key, set capture definition, get read-out list, synchronize clock).
- Scanning for new devices shall be done in one scan-cycle and not during 1 hour.

Reference

- *None*

The sequence diagram is shown in Figure 10.

Scenario 2.2: Wired binding of M-Bus using slave_install()



Comment:

New E-meter can be installed as well; results in similar process

The E-meter does not scan for new M-Bus devices for some reason.

Scans on all (unused) M-Buss addresses 0-250 for new M-Bus devices. M-Bus with scanned address replies with E5h.

Not if primary addres ≠ 0

Get Short ID

M-Bus device registered in E-meter

Report new M-Bus device to CS and get new session keys from CS

Set new user key in M-Bus device. Notice that encrypted communication is only possible when the user key is available at both sides.

Get frame counter for encrypted communication and get capture defintition

Put in DLMS object M-Bus Client Setup (Class ID: 72), attr. 3. Can be set anytime before first read-out of billing data

Read-out list with HW, SW and FW versions of M-Bus device in DLMS object M-Bus Device configuration (Class ID: 4), attr. 2

Also set clock encrypted, if it has been set before unencrypted as temporary measure, while waiting for encryption keys.

Figure 10: Sequence diagram of binding a wired M-Bus device with the slave_install() method.

8.4 Wireless configurations

8.4.1 Wireless device address

Wireless M-Bus devices must have a unique device address in the range of the M-Bus transmission. The definition of the address is provided in section 4.2.2 When the M-Bus device is installation mode, it will start periodic transmissions of installation messages (SND_IR) with the Short ID as sender address, see section 4.4.6 The selected E-meter shall respond with a confirmation message (CNF_IR) to the specific M-Bus device.

8.4.2 M-Bus Device Binding

The E-meter needs to bind the M-Bus device to the DLMS/COSEM objects. Interaction between the back office (central system) and the E-meter is through the DLMS protocol. In the following, the interaction of the application in the E-meter and the various protocols is described, followed by an installation procedure (M-Bus binding procedure; there may be more scenario's possible).

8.4.2.1 E-Meter interaction

1) The E-meter always sends a CNF_IR to a *registered* M-Bus device, after reception of a SND_IR of that *registered* M-Bus device. No further action follows, the E-meter just responds with the appropriate message;
2) An M-Bus device is called *registered* in the E-meter when the Short ID (see section 4.2.2) values are written in respective DLMS/COSEM M-Bus objects;
3) An M-Bus device is registered in the E-meter through:
    a. Manual selection from a display at the E-meter of a (unregistered) M-Bus device that sends an SND_IR message. The E-meter shall be in Installation mode to display the received serial number. The E-meter will load the M-Bus Short ID found in the SND_IR message after manual selection;
    b. Loading M-Bus device Short ID through the P0 port by means of a PDA;
    c. Loading M-Bus device Short ID through the P3 port by the CS.

8.4.2.2 Local M-Bus Binding Procedure

The binding procedure, based on manual selection on the display of the E-meter, is shown in 5. In this case it is assumed that the initial user key is set by the manufacturer and unknown by the system or E-meter. An alternative option is to configure the M-Bus device without the key set (null key).

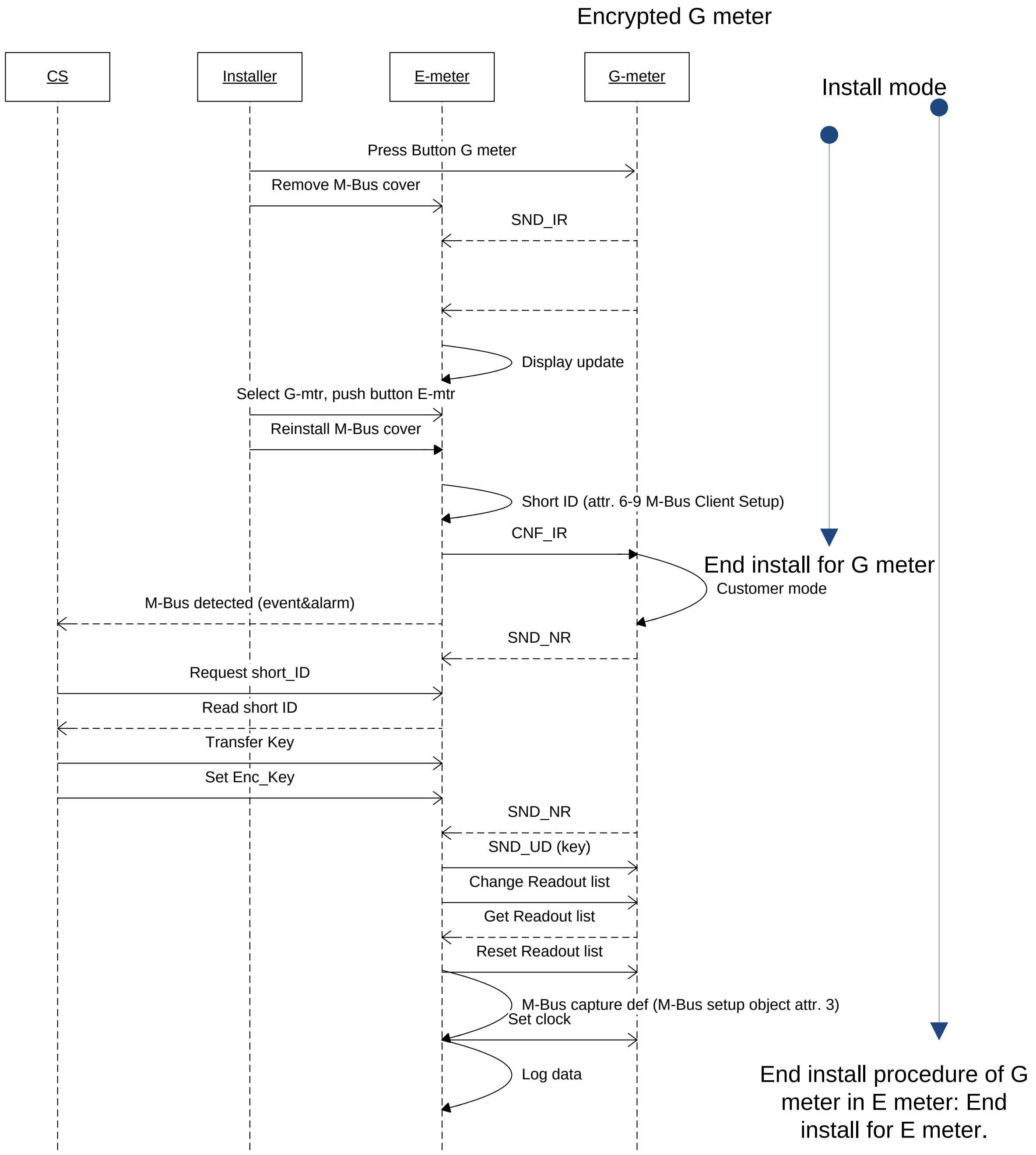


Figure 11: Example wireless binding procedure with manual selection.

Figure 11 describes how an installer manually starts the M-bus installation process by pushing a button on the gasmeter and by removing the M-bus cover on the E-meter to start the installation mode on the E-meter. The gasmeter in this example is delivered with the User-key.

The various steps are in detail:

1. The installer instructs the M-Bus device to go into Installation mode;
2. The installer removes the M-Bus cover of the E-meter;
3. The M-Bus device sends a SND_IR containing the Short ID as sender address (ref.4.2.1);
4. The M-Bus device sends out SND_IR messages every minute for a period of 60 minutes. If the M-Bus device hasn't received a CNF_IR after 60 minutes yet then the M-Bus device will continue sending SND_IR messages every hour. It must be possible to return to sending SND_IR every minute again by means of the push-button;
5. The correct M-Bus device is selected by the E-meter.
   Selecting manually the correct M-Bus device at the E-meter;
   i. The installer searches the correct M-Bus device at the display of the E-meter based on a list of (partial) Short IDs;
   ii. The installer selects the correct M-Bus device with a button action at the E-meter;
   iii. The E-meter writes the Short ID from the SND_IR message of the selected M-Bus device into the DLMS objects;
6. Once the Short ID of the M-Bus device is written in the E-meter's DLMS objects and the E-meter receives a SND_IR message of that M-Bus device, the E-meter replies with a CNF_IR;
7. The installer replaces the M-Bus cover;
8. From this moment on the M-Bus device will send regular hourly data, by sending SND_NR messages including meter reading. Notice that the keys of the M-Bus device are not yet set and unknown by the E-meter. As the clock is not set yet, the time of the first hourly transmission of the M-Bus device appears as completely random for the E-meter;
9. Upon receiving a set of keys from the CS, the E-meter shall send the encrypted key to the M-Bus device as described in section 6.5.1. There is no timing restriction on the exchange of User keys;
10. After the keys are set in both the E-meter and the M-Bus device, also the clock of the M-Bus device can be set[5];
11. The E-meter shall retrieve meter configuration data from the M-Bus device by modifying the standard readout list.

[5] The assumption here is that the M-Bus device is encrypted with an unknown (random) key at installation time. An alternative configuration option is that the M-Bus device is delivered unencrypted. In that case the time can be set directly after the first SND_NR message without setting the keys first.

After these steps the M-Bus device will send regular hourly data, by sending SND_NR messages including meter reading data. Now the keys and the clock of the M-Bus device are set and synchronised with the E-meter.

8.4.2.3 Remote wireless M-Bus binding Procedure via CS

The binding procedure is shown in figure 12. In this case it is assumed that the initial user key is set by the manufacturer and unknown by the system or E-meter. An alternative option is to configure the M-Bus device without the key set (null key).

Encrypted G meter

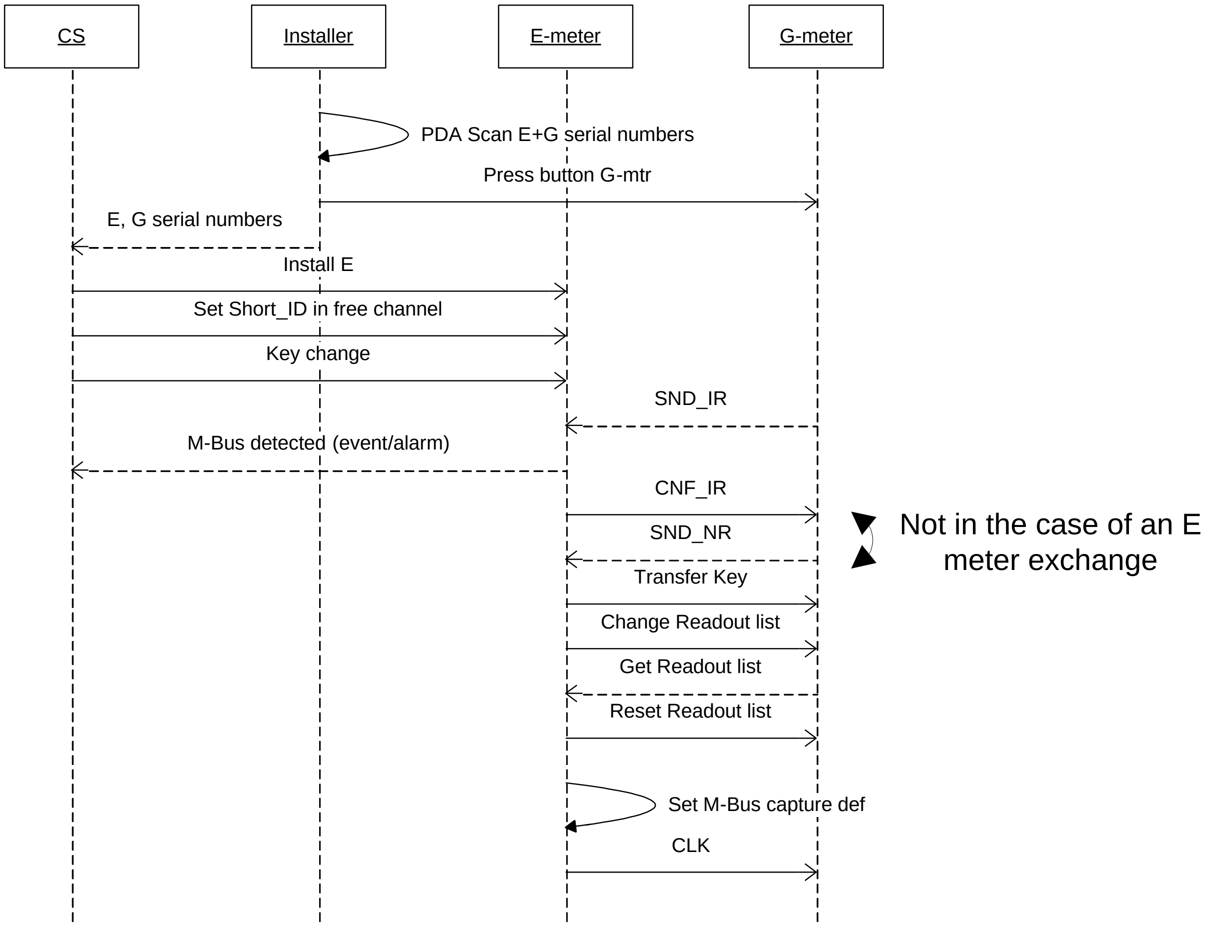


Figure 12: Example wireless binding procedure via the Central System.

This usecase describes how an installer scans the meternumbers of the E- and G-meter that are sent to the Central System (e.g. by PDA). The Central System will bind the E- and G-meter by writing attributes in the M-bus Client Setup. The gasmeter in this example is delivered with the User-key.

The various steps are in detail:

1. The installer will scan the barcodes of the E- and G-meter with the use of a PDA;
2. The installer will bring the gasmeter in installation mode by pressing the button on the gasmeter;
3. The M-Bus device sends a SND_IR containing the Short ID as sender address (ref.4.2.1);
4. The M-Bus device sends out SND_IR messages every minute for a period of 60 minutes. If the M-Bus device hasn't received a CNF_IR after 60 minutes yet then the M-Bus device will continue sending SND_IR messages every hour (It must be possible to return to sending SND_IR every minute again by means of the push-button);
5. The CS will transfer the appropriate Short ID into the E-meter by the DLMS protocol. There is no time limit on this action;
6. Once the Short ID of the M-Bus device is written in the E-meter's DLMS objects and the E-meter receives a SND_IR message of that M-Bus device, the E-meter replies with a CNF_IR;
7. From this moment on the M-Bus device will send regular hourly data, by sending SND_NR messages including meter reading data. Notice that the keys of the M-Bus device are not set yet and unknown by the E-meter. As the clock is not yet set, the time of the first hourly transmission of the M-Bus device appears as completely random for the E-meter;
8. Upon receiving a set of keys from the CS, the E-meter shall send the encrypted key to the M-Bus device as described in section 6.5.1. There is no timing restriction on the exchange of User keys;
9. After the keys are set in both the E-meter and the M-Bus device, also the clock of the M-Bus device can be set[6];
10. The E-meter shall retrieve meter configuration data from the M-Bus device by modifying the standard readout list.

After these steps, the M-Bus device will send regular hourly data, by sending SND_NR messages including meter reading data. Now the keys and the clock of the M-Bus device are set and synchronised with the E-meter.

8.4.2.4 Remote binding proces in case the E-meter is replaced

This scenario handles the process of binding a wireless G-meter (in general a M-Bus device) to an E-meter which is not bound yet to this M-Bus device.

[6] The assumption here is that the M-Bus device is encrypted with an unknown (random) key at installation time. An alternative configuration option is that the M-Bus device is delivered unencrypted. In that case the time can be set directly after the first SND_NR message without setting the keys first.

Trigger	Description
Exchange Measuring equipment	During installation of the Measuring equipment, the manual wireless M-Bus installation process through buttons on the E-meter is not executed, e.g. the M-Bus cover has not been opened.
Corrective action by Operations	For refreshing settings in the CS or Measuring equipment, Operations remotely de-installs and reinstalls the M-Bus device.

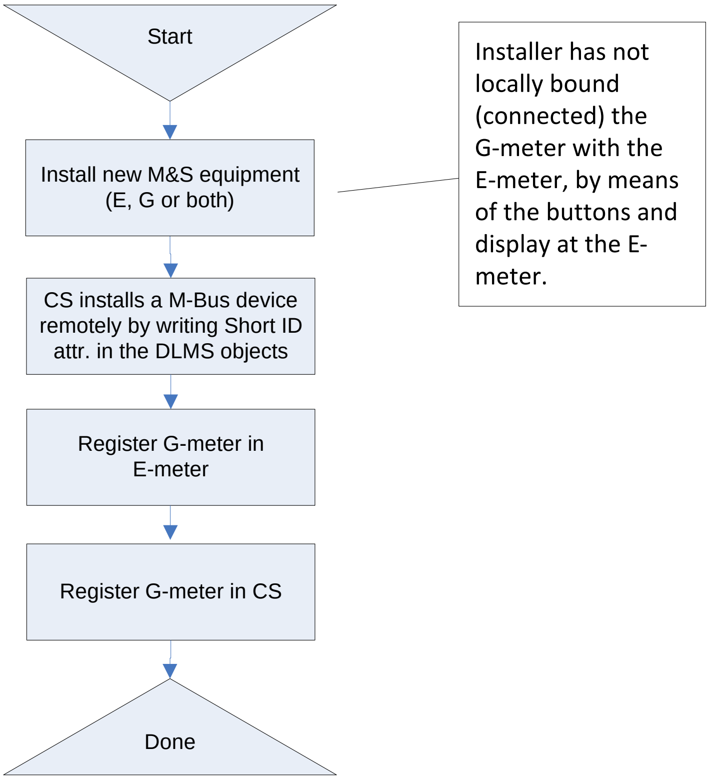

Start
Install new M&S equipment (E, G or both)
CS installs a M-Bus device remotely by writing Short ID attr. in the DLMS objects
Register G-meter in E-meter
Register G-meter in CS
Done
Installer has not locally bound (connected) the G-meter with the E-meter, by means of the buttons and display at the E-meter.

Figure 13: Wireless: Configuring DLMS M-Bus attributes in E-meter

Pre-conditions

- The E-meter is not bound to the transmitting M-Bus device;
- The M-Bus device is in one of the following states:
  - Installation Mode: Binding has not yet been performed but the G-meter is activated, sending installation requests (SND_IR) periodically;
  - Customer or Test Mode: the G-meter is activated, sending normal hourly data transmissions (SND_NR);
- The M-Bus device might be encrypted; in that case the key will be unknown to the E-meter.

Parameters

- DLMS M-Bus Client Setup (Class ID: 72) in the E-meter,
  specifically the Short ID attributes.

Post-conditions

- Binding of E-meter and wireless M-Bus device

Assumptions

- After transferring the keys by the CS, the E-meter shall autonomically set the capture definition, change and get the read-out list and set the clock.

Reference

- *None*

The sequence diagram is shown in Figure 14.

Scenario 2.3: Binding of wireless M-Bus with M-Bus attributes

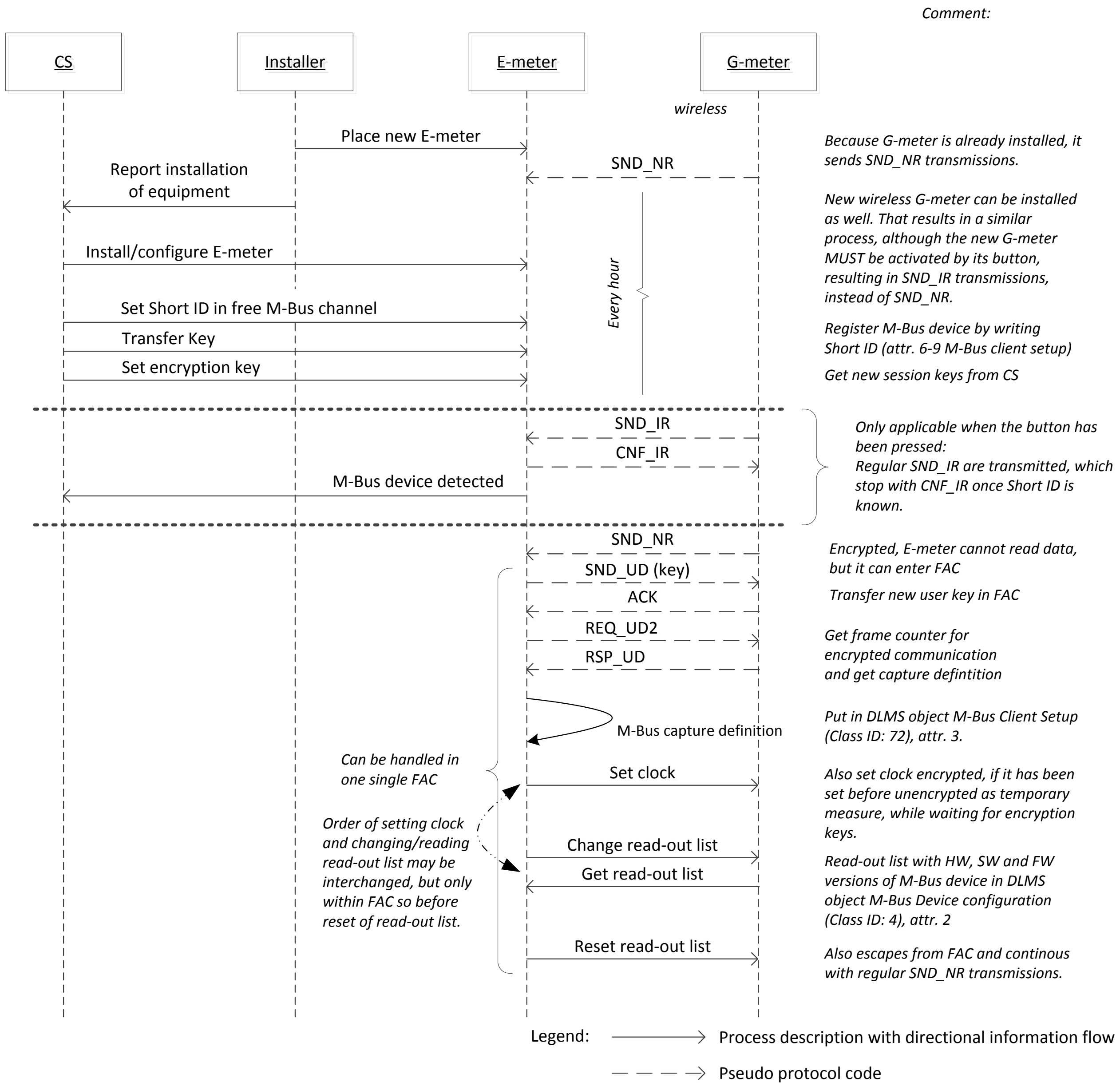

Comment:
CS
Installer
E-meter
G-meter
wireless
Place new E-meter
SND_NR
Because G-meter is already installed, it sends SND_NR transmissions.
Report installation of equipment
New wireless G-meter can be installed as well. That results in a similar process, although the new G-meter MUST be activated by its button, resulting in SND_IR transmissions, instead of SND_NR.
Install/configure E-meter
Every hour
Set Short ID in free M-Bus channel
Register M-Bus device by writing Short ID (attr. 6-9 M-Bus client setup)
Transfer Key
Set encryption key
Get new session keys from CS
SND_IR
CNF_IR
Only applicable when the button has been pressed:
Regular SND_IR are transmitted, which stop with CNF_IR once Short ID is known.
M-Bus device detected
SND_NR
Encrypted, E-meter cannot read data, but it can enter FAC
SND_UD (key)
ACK
Transfer new user key in FAC
REQ_UD2
RSP_UD
Get frame counter for encrypted communication and get capture defintition
M-Bus capture definition
Put in DLMS object M-Bus Client Setup (Class ID: 72), attr. 3.
Can be handled in one single FAC
Set clock
Also set clock encrypted, if it has been set before unencrypted as temporary measure, while waiting for encryption keys.
Order of setting clock and changing/reading read-out list may be interchanged, but only within FAC so before reset of read-out list.
Change read-out list
Get read-out list
Read-out list with HW, SW and FW versions of M-Bus device in DLMS object M-Bus Device configuration (Class ID: 4), attr. 2
Reset read-out list
Also escapes from FAC and continous with regular SND_NR transmissions.
Legend:
Process description with directional information flow
Pseudo protocol code

Figure 14: Sequence diagram of binding a wireless M-Bus device with M-Bus attributes.

9 BACKWARDS COMPATIBILITY

9.1 DSMR4.2 E meter with DSMR4.0 and DSMR4.2.1 G meter

The E-Meter behavior:

- E-Meter will not send any valve commands (not part of DSMR 4.2.2 specification).
- E-Meter accepts status information in P2 telegrams as specified in DSMR 4.0 about valve status. The information is discarded in the E-Meter:

  Gas valve specific data blocks

  Valve status

Field	Hex	Remark
DIF	89h	2 digit BCD
DIFE	40h	Valve (new definition)
VIF	FDh	Valve (new definition)
VIFE	1Ah	Digital status
Mask	XXh	02: valve released, not open 01: valve opened, 00: valve closed

- E-Meter will handle the valve capability information as specified in the Meter Configuration Data (see section   6.4.8 and P2-P3 mapping)
- A possible valve alarm (bit 7 in status field; see section 6.3.3 of this specification and the definition in DSMR 4.0) will be ignored .

The G-Meter behavior:
The DSMR4.2.2 E-meter will not send valve commands therefore the G-Meter will not receive any valve commands.; it just behaves according DSMR 4.0 specification

9.2 DSMR4.0 E meter with DSMR4.2.2 G meter

The E-Meter behavior:

- The E-Meter receives the valve capabilities of the G-meter in the Meter Configuration Data (see section   6.4.8 and P2-P3 mapping). The capabilities will indicate that the G-Meter does not have a valve.

The G-Meter behavior:

- G-Meter does not have a valve and indicates that in the Meter Configuration Data (see section   6.4.8).

10 DOCUMENT LIST

Following table shows the complete set of documents that build up the Dutch Smart Meter Requirements, of which this Companion standard P2 document is a part of.

Document name postfix	Description
Main	The main document of the Dutch Smart Meter Requirements, containing all definitions and most of the use cases and requirements
P1	Companion standard P1
P2	Companion standard P2
P3	Companion standard P3
GPRS	Additional document describing the requirements for the GPRS infrastructure as part of the Dutch Smart Meter Specification.

APPENDIX A: P2 – P3 MAPPING

DIF	DIFE	VIF	VIFE	Value	Section	P3 reference	
				M-Bus Client Setup object	**4.2.3**	**0-x.24.1.0.255-** (version)	
0Dh		78h		Equipment identifier	**6.4.1**	P3 section 7.2 **0-x:96.1.0.255** (x=channel number (1..4))	Set by manufacturer, read-only. This is a 17 byte field.
0Ch		13h		Gas meter reading, converted	**6.4.3**	**0-x:24.3.0.255** (x=channel number (1..4)) Capture_Objects	
0Ch		14h		Gas meter reading, converted (G10-G25)	**6.4.3**	**0-x:24.3.0.255** (x=channel number (1..4)) Capture_Objects	
0Ch		93h	3Ah	Gas meter reading, unconverted	**6.4.3**	**0-x:24.3.0.255** (x=channel number (1..4)) Capture_Objects	
0Ch		94h	3Ah	Gas meter reading, unconverted (G10-G25)	**6.4.3**	**0-x:24.3.0.255** (x=channel number (1..4)) Capture_Objects	
0Ch		0Dh		Heat Meter Reading	**6.4.5**	**0-x:24.3.0.255** (x=channel number (1..4)) Capture_Objects	
4Ch		0Dh		Cold meter reading	**6.4.6**	**0-x:24.3.0.255** (x=channel number (1..4)) Capture_Objects	
0Ch		13h		Heat meter reading Volume	**6.4.6**		
0Ch		13h		Water meter reading	**6.4.7**	**0-x:24.3.0.255** (x=channel number (1..4)) Capture_Objects	
01h		FDh	67h	Meter Configuration Mask	**6.4.78**	**0-x:24.3.0.255** (x=channel number (1..4)) Capture_Objects	
01h		7Ah		M-Bus Device Address	**6.2.2**	**0-x:24.1.0.255** primary_address	
0x07 0x47		FDh	19h	Encrypted user key	**4**		
01h		FDh	17h	Status	**6.3.3**	**0-x:24.1.0.255** – status	Use DIF/VIF in Read Out List, not in the Status byte

Header Data (ref 4.3.2 and 0)

M-Bus Field name	P3 reference
Ident Number	**0-x:24.1.0.255** - identification_number
Manufacturing ID	**0-x:24.1.0.255** – manufacturer_id

Version	**0-x:24.1.0.255** – version
Medium	**0-x:24.1.0.255** – device_type
Access Number	**0-x:24.1.0.255** – access_number
Status – alarm flags	**Not used**
Configuration – Encryption method	None

APPENDIX B: MESSAGE EXAMPLES

All examples in this document use the following values:

- Equipment Identifier is ’XXXXX110123456789’
- Identification Number is ‘23456789’
- Manufacturer Identification is ‘NET’ (hex): 38 B4
- Version Identification is the DSMR 4.2 (42h)
- Device Type identification is gas (03h)
- Default Key (hex): 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
- User Key (hex): 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
- Frame Counter (hex): 00 00 00 01
- Examples with encryption method = 0x0F use the following initialization vector (hex): B4 38 89 67 45 23 40 03 01 00 00 00 01 00 00 00

B1 Wired telegrams

Below the template for wired telegrams can be found.

Field		Hex	Remark
	Start Character	68h	Start byte long telegram
	L	L-0	Length
	L	L-0	Length
	Start Character	68h	Start byte long telegram
	C	53h / 73h	FCB=0 / FCB = 1
	A	A-0	Primary Address
	CI	5Ah	Data send (master to slave)
4 byte data header	Access No	AC-0	Access Number
	Status	S-0	Not used
	Configuration	X0	Number of bytes encrypted, must be multiple of 16
		EC-0	Encryption Method Code
Variable Data Blocks (including filler bytes)			
DIF		04h	4 Bytes integer LSB of the sum of data fields 4 - 11
VIF		FDh	a VIFE follows
VIFE		08h	unique telegram identification (Frame counter)
		XXh	

Field		Hex	Remark
		XXh	
		XXh	
		XXh	
CS		XXh	Checksum
Stop Char-acter		16h	Always 16H

B1.1 Example Key change

The User Key is encrypted with the Default Key: 27 9F B7 4A 75 72 13 5E 8F 9B 8E F6 D1 EE E0 03

Note : The encrypted data is split in two blocks of 8 octets:

Block containing the MSB: 27 9F B7 4A 75 72 13 5E
Block containing the LSB: 8F 9B 8E F6 D1 EE E0 03

Field	Hex	Remark
Start Character	68h	Start byte long telegram
L	19h	Length
L	19h	Length
Start Character	68h	Start byte long telegram
C	53h	(FCB=0)
A	01h	Primary Address
CI	51h	Data send (master to slave)
DIF	07h	64 bit data, Storage 0
VIF	FDh	VIF from table 11
VIFE	19h	Reserved -> AES 128 KEY exchange
User Key 1	03h	Block containing the LSB (LSB first)
User Key 2	E0h	
User Key 3	EEh	
User Key 4	D1h	
User Key 5	F6h	
User Key 6	8Eh	
User Key 7	9Bh	
User Key 8	8Fh	
DIF	47h	64 bit data, Storage 0
VIF	FDh	VIF from table 11
VIFE	19h	Reserved -> AES 128 KEY exchange
User Key 9	5Eh	Block containing the MSB (LSB first)

Field	Hex	Remark
User Key 10	13h	
User Key 11	72h	
User Key 12	75h	
User Key 13	4Ah	
User Key 14	B7h	
User Key 15	9Fh	
User Key 16	27h	
CS	4Eh	Checksum
Stop Character	16h	Always 16

B1.2 Example Retrieve version information

1. Selecting the data to retrieve (Hardware and Metrology version)

Request		
Field	Hex	Remark
Start	68h	
Length	1Ah	
Length	1Ah	
Start	68h	
C field	53h	Send user data to slave (SND_UD)
Address	--	Primary address
CI field	5Ah	Data send master to slave (encrypted)
Access No	01h	Access Number
Status	00h	
Configuration word	10h 05h	
DIF	08h	Request for readout (Hardware version #)
VIF	FDh	
VIFE	0Dh	
DIF	08h	Request for readout (Metrology (firmware) version #)
VIF	FDh	
VIFE	0Eh	
Filler bytes	2Fh 2Fh 2Fh 2Fh 2Fh 2Fh 2Fh	

	2Fh 2Fh 2Fh	
DIF	04h	unique telegram identification (Frame counter)
VIF	FDh	
VIFE	08h	
	--	
	--	
	--	
	--	
CS	--	Check sum
Stop Character	16h	Always 16H

Response		
Field	Hex	Remark
Start character	E5h	The slave returns a single Character E5 = OK

2. Requesting the data

Request		
Field	Hex	Remark
Start	10h	Short form M-Bus message
C field	5Bh	REQ_UD2
Address	--	Primary address
CS	--	Check sum
Stop Character	16h	Always 16H

Response		
Field	Hex	Remark
Start	68h	Start byte Long Telegram
L	4Ah	Length xx Bytes
L	4Ah	Length xx Bytes
Start	68h	Start byte
C	08h	Sending of the required data
A	--	Primary address or 253 for secondary address
CI	72h	Answer of variable length
Ident. Nr. 4 Byte	78h	Ident Number, e.g. 12345678 in BCD
	56h	
	34h	
	12h	

Manfacturer ID	--	
	--	
Version	42h	DSMR compliance level
Medium	03h	Medium, e.g. Gas
Access Nr	--	Access Counter (obsolete)
Status	00h	Not used
Configuration Word	40h	Encryption size == 4 blocks
	0Fh	Encryption method (default AES)
DIF	0Dh	Variable length string
VIF	FDh	Hardware version number
VIFE	0Ch	
LVAR	1Bh	Length = 27
8 bit string (LSB first)	0Ah	LF
	0Dh	CR
	72h	r
	65h	e
	69h	i
	6Ch	l
	70h	p
	70h	p
	75h	u
	73h	s
	20h	
	65h	e
	6Ch	l
	75h	u
	64h	d
	6Fh	o
	6Dh	m
	20h	
	73h	s
	75h	u
	62h	b
	2Dh	-
	4Dh	M
	3Dh	=
	6Dh	m
	6Fh	o
	63h	c
DIF	0Dh	Variable length string
VIF	EDh	Metrology (firmware) version number
VIFE	0Ch	
LVAR	0Fh	Length = 15
8 bit string (LSB first)	0Ah	LF

	0Dh	CR
	35h	5
	2Eh	.
	34h	4
	2Eh	.
	33h	3
	32h	2
	31h	1
	57h	W
	46h	F
	3Dh	=
	74h	t
	65h	e
	6Dh	m
Filler bytes	2Fh 2Fh 2Fh 2Fh 2Fh 2Fh 2Fh 2Fh 2Fh 2Fh 2Fh 2Fh 2Fh 2Fh	
DIF	04h	unique telegram identification (Frame counter)
VIF	FDh	
VIFE	08h	
	--	
	--	
	--	
	--	
CS	--	Checksum
Stop	16h	Stop

3. Resetting the request list

Request		
Field	Hex	Remark
Start	10h	Short form M-Bus message
C field	40h	SND_NKE

Address	--	Primary address
CS	--	Check sum
Stop Character	16h	Always 16H

Response		
Field	Hex	Remark
Start character	E5h	The slave returns a single Character E5 = OK

B1.3 RSP_UD telegram of a Gas Meter

This example shows a RSP_UD telegram (before encryption) of a meter comprising of the following properties:

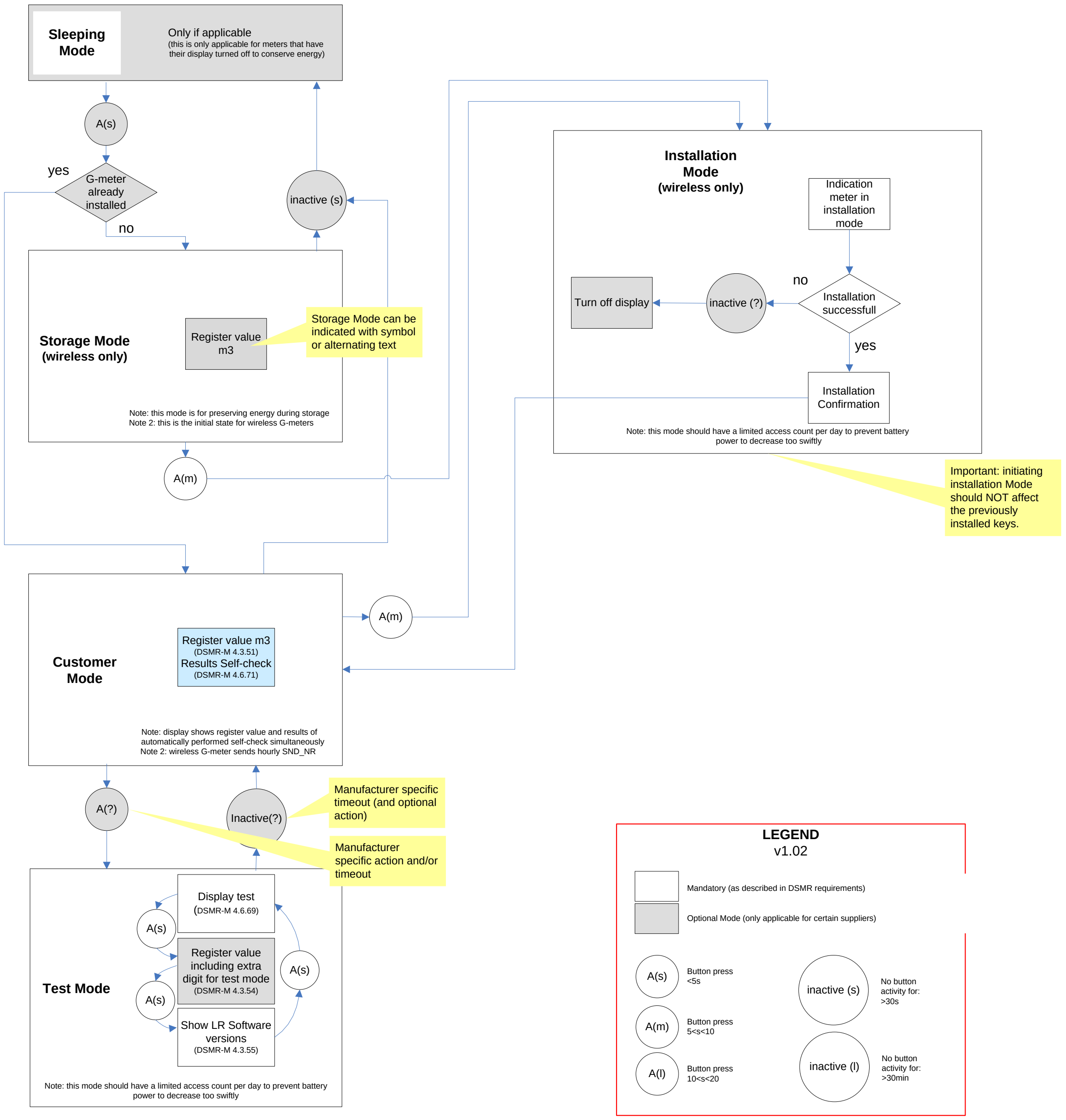
- temperature converted volume
- meter type G4 => volume multiplier = 0,001m³

Field	**Hex**		**Remark**
	clear	**encrypted**	
Start Character	68		
L	3F		
L	3F		
Start Character	68		
C	08		RSP_UP
A	01		
CI	72		
Identification Number	89		ID: ‘23456789’
	67		
	45		
	23		
Manufacturer Identification	B4		’NET’
	38		
Version Ident.	42		DSMR compliancy level, i.e. 4.2
Device type	03		Medium, eg. gas
Access No	F6		
Status	00		Not used
Configuration Word	00	30	48 encrypted bytes.
	00	0F	Mode 15, AES 128 bit encryption
Encryption Verification	2F	F1	2 Idle Filler bytes
	2F	80	
DIF	01	C5	8 bits
VIF	FD	3E	Use VIFE

Field	Hex		Remark
	clear	encrypted	
VIFE	17	07	Error flags
Status byte	00	68	Encrypted Status
DIF	0D	C7	variable length
VIF	78	6A	Serial number
LVAR	11	E6	Serial number length 17 Field
Equipment Identifier	39	E2	'XXXXX110123456789'
	38	4A	
	37	98	
	36	BD	
	35	D5	
	34	94	
	33	7F	
	32	62	
	31	27	
	30	32	
	31	BF	
	31	63	
	58	72	
	58	AA	
	58	2A	
	58	A9	
	58	AF	
DIF	46	6D	6 bytes integer, storage bit set
VIF	6D	0F	Date and Time data type I
Time stamp	00	0C	Date/Time (yy.mm.dd hh:mm:ss) = 09.06.18 11:00:00
	00	71	
	0B	FB	
	32	59	
	16	7F	
	00	FC	
DIF	4C	62	8 digit BCD storage 1
VIF	13	05	Volume (0,001 m^3)
Meter value (converted volume)	91	A2	'00000391'
	03	5F	
	00	50	
	00	84	
DIF	01	27	1 digit binary
VIF	FD	87	Extension
VIFE	67	A6	Special Supplier Information

Field	Hex		Remark
	clear	encrypted	
Meter Configuration	05	F0	- clock, temp corrected
Idle Filler	2F	C2	Idle Filler
	2F	9D	
Encryption Verification	2F	50	2 Idle Filler bytes
	2F	7B	
DIF	04		4 Bytes integer (unencrypted)
VIF	FD		a VIFE follows
VIFE	08		Frame counter
	01		E.g start with 00 00 00 01 (LSB first)
	00		
	00		
	00		
CS	53	93	Checksum (unencrypted)
Stop Character	16		

APPENDIX C: ONE BUTTON PROCESS


Sleeping Mode
Only if applicable
(this is only applicable for meters that have their display turned off to conserve energy)
A(s)
yes
G-meter already installed
no
inactive (s)
Storage Mode (wireless only)
Register value m3
A(m)
Installation Mode (wireless only)
Indication meter in installation mode
no
Installation successfull
yes
Installation Confirmation
inactive (?)
Turn off display
Customer Mode
Register value m3
(DSMR-M 4.3.51)
Results Self-check
(DSMR-M 4.6.71)
A(m)
A(?)
Inactive(?)
Test Mode
Display test
(DSMR-M 4.6.69)
A(s)
Register value including extra digit for test mode
(DSMR-M 4.3.54)
A(s)
A(s)
Show LR Software versions
(DSMR-M 4.3.55)
LEGEND
v1.02
Mandatory (as described in DSMR requirements)
Optional Mode (only applicable for certain suppliers)
A(s)
Button press <5s
A(m)
Button press 5<s<10
A(l)
Button press 10<s<20
inactive (s)
No button activity for: >30s
inactive (l)
No button activity for: >30min

Storage Mode can be indicated with symbol or alternating text

Note: this mode is for preserving energy during storage
Note 2: this is the initial state for wireless G-meters

Note: this mode should have a limited access count per day to prevent battery power to decrease too swiftly

Important: initiating installation Mode should NOT affect the previously installed keys.

Note: display shows register value and results of automatically performed self-check simultaneously
Note 2: wireless G-meter sends hourly SND_NR

Manufacturer specific timeout (and optional action)

Manufacturer specific action and/or timeout

Note: this mode should have a limited access count per day to prevent battery power to decrease too swiftly