Elster GmbH
R&D Residental Gas Metering
Strotheweg 1
49504 Lotte (Büren)

T: +49 (0)541/1214-0
F: +49 (0)541/1214-370

P2 v2.2 Elster Implementation

AE.02:01.01:01.01

Specification

Version:	v01.08
State:	released
Date:	22.02.2010
Author:	Wilfried Többen
Phone:	+49 (0)541/1214-119

Revision history

Date:	Version:	Author:	Description:
02.11.2009	0.1	Többen	Initial version
02.11.2009	1.0	Többen	Released
16.11.2009	1.01	Többen	Annex B.6, Example 8 removed (not applicable) Annex B.11, Example 16 corrected
26.11.2009	1.02	Többen	Chapter 4.1: Clear definition, how the E-Meter determines the appropriate encryption method. Chapter 4.1.1: Clear definition, which system uses which encryption method. Chapter 4.5.2, Notes 1 and 2: Hints added to make clear, what kind of devices are meant (Encoder or ACM WAVE SYSTEM)
08.12.2009	1.03	Többen	Annex B.11, Reference to Example 15 corrected. Index corrected.
12.01.2010	1.04	Többen	Versionstring on first page
18.01.2010	1.05	Többen	Definition of RSP_UD Standard Data Record in 4.5.9 corrected: “Encryption Verification” added.
20.01.2010	1.06	Többen	Chapter 4.2.1 and 4.3.4: Added a note that bit 5 shall be set if the time sync command is later than the last one (according to SOW document, version 1.0)
10.02.2010	1.07	Többen	Added notes to sections 3.1.5 and 3.1.6.
22.02.2010	1.08	Többen	Chapter 4.3.4: Set and Reset conditions for Error Bit 5 updated: this bit is managed by both, the Encoder as well as the Wave System (see also version 1.05)

Contents

1 Introduction

The document describes the implementation of the M-Bus protocol for Elster devices as specified in DSMR P2 v2.2. It specifies the P2 protocol for wired M-Bus connections and for dongle based connections.
The wireless M-Bus connection is out of scope of this document.

1.1 Keys

All examples in this document use the following keys:

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
```

Examples with encryption method = 0x05 use the following initialization vector:

```
93 15 78 56 34 12 33 03 01 01 01 01 01 01 01 01
```

2 Physical Layer

Baud rate	2400
Parity	Even
Data Bits	8
Stop Bit	1
Max. number of M-Bus slaves	4
Max. current per M-Bus slave	6 mA (4*1,5 mA)

Table 1 M-Bus Interface Configuration

3 Data Link Layer

The usage of the frame count bit (FCB) of the C-Field is specified in [2]. The assumption is that ignoring the FCB in the particular case of P2 communication has no harming side-effect, since communication is carried out with single, independent, packets.

3.1 C-Fields Overview

Name	Hex
SND_NKE	40
REQ_UD1	5A
REQ_UD2	5B
SND_UD	53
RSP_UD	08

Table 2: C-Fields Overview

3.1.1 SND_NKE

	Field	Hex	Remark
0	Start Character	10	Sort frame
1	C-Field	40	SND_NKE
2	A	A-0	Primary Address
3	*Checksum*		
4	Stop Character	16	

Table 3:SND_NKE

3.1.2 REQ_UD1

	Field	Hex	Remark
0	Start Character	10	Start byte sort telegram
1	C	5A	Request User Data (counter sending) FCB=0
2	A	A-0	Primary Address
3	*Checksum*		
4	Stop Character	16	Always 16

Table 4:REQ_UD1

3.1.3 REQ_UD2

	Field	Hex	Remark
0	Start Character	10	Start byte sort telegram
1	C	5B	Request User Data (counter sending) FCB=0
2	A	A-0	Primary Address
3	*Checksum*		
4	Stop Character	16	Always 16

Table 5:REQ_UD2

3.1.4 SND_UD

	Field	Hex	Remark
0	Start Character	68	Start byte long telegram
1	L	L-0	Length
2	L	L-0	Length
3	Start Character	68	Start byte long telegram
4	C	53	SND_UD (FCB=0)
5	A	A-0	Primary Address
6	*CI-Field Data Block*		
7	*Checksum*		
8	Stop Character	16	Always 16

Table 6: SND_UD

Note 1: The reception of SND_UD telegrams is confirmed by the link layer with a single byte 0xE5. The application layer might need more time for processing the received telegram. During this time, the power supply of the M-Bus device must **not** be switched off. In order to ensure that the telegram is completely processed, the M-Bus Master shall send subsequent REQ_UD1 telegrams until it receives another 0xE5.

3.1.5 RSP_UD

	Field	Hex	Remark
0	Start Character	68	Start byte long telegram
1	L	L-0	Length
2	L	L-0	Length
3	Start Character	68	Start byte long telegram
4	C	08	(FCB=0)
5	A	A-0	Primary Address
6	*CI-Field Data Block*		
7	*Checksum*		
8	Stop Character	16	Always 16

Table 7: RSP_UD

Note 1: Within the ACM WAVE SYSTEM RF, the TRANSMITTER transfers the Gas Meter volume periodically (period ‘p’) to the RECEIVER. The emission is performed at a randomized point in time during the given period ‘p’. The RECEIVER stores each RSP_UD for at least p/2. In order to capture every periodic readout volume, the M-Bus Master shall perform at least one REQ_UD2 within p/2.

Example:
If the readout period p is 60 minutes, the M-Bus Master shall perform a REQ_UD2 at least every 30 minutes.

4 Application Layer

4.1 Data Encryption

This guideline for P2 communication allows for two methods of encryption, both based on AES-128. The Master shall determine the appropriate method based on the response of the Slave. The identification of the encryption method is based on the RSP_UD telegram in response of a REQ_UD2 request. The implication is that the Master cannot send encrypted messages to the Slave before it has receives one first.

- When **decrypting** received telegrams (slave to master), the master shall determine the appropriate method from the signature field.

- When **encrypting** telegrams that shall be transferred to the slave, the master shall determine the appropriate method from the data point 'Meter Configuration Data', bit 'Clock Device Implemented' (see also chapter 4.4.10), which can be found in the previously received response of the slave (see Table 8). If there is no 'Meter Configuration Data', only unencrypted messages can be sent, i.e. setting M-bus address; setting key; request for user data.

	Bit 'Clock Device Implemented'	Encryption Method
0	0	05h
1	1	04h

Table 8: Determining Encryption Methods

4.1.1 Encryption Method

	Encryption Method Code (header signature field)	Algorithm	Key size	Status	
				E-Meter	G-Meter
0	00xxh	None (no encryption)	-	M	M
1	02xxh	DES	64	n. a.	n. a.
2	03xxh	DES	64	n. a.	n. a.
3	04xxh	AES-128, CBC Mode 4	128	M	C1
4	05xxh	AES-128, CBC Mode 5	128	M	C2

Table 9: Encryption Method Codes

M = Mandatory
C = Conditional

Condition C1: Mandatory for devices with a clock, i.e. Encoder with ACM WAVE SYSTEM.
Condition C2: Mandatory for devices without a clock, i.e. Encoder with ACM WIRED M-BUS.

4.1.2 Initialization Vector

4.1.2.1 Encryption Method Code = 04h

The Initialization Vector for Encryption Method Code = 04h is always:

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

4.1.2.2 Encryption Method Code = 05h

The Initialization Vector for Encryption Method Code = 05h is constructed as follows:

	Field	Hex	Remark
0	Manufacturer ID	MI-0	Manufacturer ID of the M-Bus slave.
1		MI-1	
2	Identification ID	ID-0	Identification Number of the M-Bus slave.
3		ID-1	
4		ID-2	
5		ID-3	
6	Version	V-0	Version of the M-Bus slave
7	Medium	M-0	Medium of the M-Bus slave
8	Access Counter	AC-0	Access Counter; related to the current telegram containing this data repeated 8 times
9	Access Counter	AC-0	
10	Access Counter	AC-0	
11	Access Counter	AC-0	
12	Access Counter	AC-0	
13	Access Counter	AC-0	
14	Access Counter	AC-0	
15	Access Counter	AC-0	

Table 10: Initialization Vector, Encryption Method Code = 05h

Note 1: The one byte access counter is used as fill character in the high order bytes 8 to 15, i.e. it is repeated 8 times.

Note 2: The access counter has the same value as specified in the (unencrypted) header of the telegram that contains this data.

Example 1 shows an Initialization Vector as it might be sent to and from a slave.

	Field	Hex	Remark
0	Manufacturer ID	93	Manufacturer ID e.g. “ELS”
		15	
1	Identification ID	78	Identification Number, e.g. 12345678
		56	
		34	
		12	
2	Version	33	Version e.g. 51
3	Medium	03	Medium, e.g. gas
4	Access Counter	01	Access Counter of the current telegram
5	Access Counter	01	
6	Access Counter	01	

	Field	Hex	Remark
7	Access Counter	01	
8	Access Counter	01	
9	Access Counter	01	
10	Access Counter	01	
11	Access Counter	01	

Example 1: Initialization Vector

4.1.3 Encryption Verification

In order to verify the encryption, the first data block of each encrypted telegram shall contain specific data. After successful decryption, this specific data shall be recognized.
If the encryption verification fails (i.e. the specific data is not recognized), the error status code “Fraud Attempt” shall be set (see 4.3.4).

4.1.3.1 Encryption Method Code = 04h

The first data block of the encrypted part of any telegram will be the date & time value of the sender to ensure that the first block contains a changing element.

	Field	Hex	Remark
0	DIF	06	6 Bytes Integer
1	VIF	6D	Extended Date and Time compound data type I
2	Meter Clock Time	T-0	current meter clock time
3		T-1	
4		T-2	
5		T-3	
6		T-4	
7		T-5	

Table 11: Encryption Verification, Encryption Method Code = 04h

4.1.3.2 Encryption Method Code = 05h

The first block of the encrypted part of any telegram will hold two filler bytes containing the value 2FH.

	Field	Hex	Remark
0	DIF	2F	Encryption Verification
1	DIF	2F	

Table 12: Encryption Verification, Encryption Method Code = 05h

4.2 Protection against replay attacks

The AMI system shall be protected against replay attack, including replay attack at the P2 communication. Without measures, an attacker may fake meter readings by recording and replaying original P2 communication messages and the Master or AMI system will not be able to detect this type of fraud. This attack will lead to incorrect billing data and needs to be prevented. The following will describe a method to prevent replay attack.

4.2.1 Encryption Method Code = 04h

When decrypting data, the date time value in the telegram shall be later than the date time value of the last transmission. If the value is equal or less (earlier) then the telegram is discarded. A “Clock synchronization error” (bit 5) is reported by the G-meter in the status field. This protects the receiver against replay attacks.

Both the Master and Slave will accept encrypted message with any date time value after the user key of the Slave has been changed.

If the Master (E-meter) has set the time, the following message from the Slave (G-meter) shall have a date time value later than this set time command. If the Master detects a value equal or less (i.e. earlier), the telegram is discarded.

Note: the consequence of this protection mechanism is that the maximum frame rate limited to one frame per second.

4.2.2 Encryption Method Code = 05h

Any date & time value in both directions is ignored and every correctly decoded message is accepted.

4.3 CI-Fields Overview

Control Information	Hex
Application Reset	50
Command to device	51
Selection of device	52
Command to device, Short Data Header	5A
Command to device, Long Data Header	5B
Response from device, Fixed Data Header	72

Table 13: CI-Fields Overview

4.3.1 Short Data Header

	Field		Hex	Remark
0	*SND_UD Frame*			
1		CI	5A	Data send (master to slave)
2	4 byte data header	Access No	AC-0	Access Number
3		Status	S-0	Status
4		Signature	X0	Number of bytes encrypted, must be multiple of 16
5			EC-0	Encryption Method Code, see chapter 4.1.1
6	*Variable Data Blocks*			

Table 14: Short Data Header (CI=5Ah)

4.3.2 Long Data Header

	Field			Hex	Remark
0	*SND_UD Frame*				
1			CI	5B	Data send (master to slave)
2	Long Data Header	Short ID	Identification Number	ID-0	Identification Number
3				ID-1	
4				ID-2	
5				ID-3	
6			Manufacturer Identification	MI-0	Manufacturer ID
7				MI-1	
8			Version	V-0	Generation
9			Medium	M-0	Medium
10		Short Header	Access No	AC-0	Access Number
11			Status	ST-0	Error Status Code
12			Signature	X0	Number of bytes encrypted, must be multiple of 16
13				EC-0	Encryption Method Code, see chapter 4.1.1
14	*Variable Data Blocks*				

Table 15: Long Data Header

4.3.3 Fixed Data Header

	Field			Hex	Remark
0	*RSP_UD Frame*				
1			CI	72	Data send (slave to master)
2	Fixed Data Header	Short ID	Identification Number	ID-0	Identification Number
3				ID-1	
4				ID-2	
5				ID-3	
6			Manufacturer Identification	MI-0	Manufacturer ID
7				MI-1	
8			Version	V-0	Generation
9			Medium	M-0	Medium
10		Short Header	Access No	AC-0	Access Number
11			Status	ST-0	Error Status Code
12			Signature	X0	Number of bytes encrypted, must be multiple of 16
13				EC-0	Encryption Method Code, see chapter 4.1.1
14	*Variable Data Blocks*				

Table 16: Fixed Data Header

Note 1: The combination of Identification Number (4 octets), Manufacturer identification (2 octets), Version identification (1 octet) and Device Type identification (Medium field, 1 octet) is defined as the Short ID.

Note 2: The Short ID shall be unique within the network of the grid operator. The manufacturer guarantees uniqueness with a Version field that is fixed over the lifetime of the individual M-bus device. Hence firmware upgrades are not possible without changing the Version number.

Note 3: The Identification Number is derived from the Equipment Identifier as specified in chapter 4.4.5. 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.

4.3.4 Error Status Codes

The Error Status code is implemented as a bit mask:

$b_7\ b_6\ b_5\ b_4\ b_3\ b_2\ b_1\ b_0$

	Bit	Meaning	Set Conditions	Reset Conditions
0	b_0	Application Busy	The communication between the Encoder and the Transmitter does not work.	The Wave Transmitter received a new SND_UD.
1	b_1	Any Application Error	The Encoder was not able read the Index.	A new user key is set.
2	b_2	Power low	At least one battery (Wave Transmitter, Wave Repeater) is going low.	Never.
3	b_3	Permanent error	n.a.	n.a.
4	b_4	Temporary error	Communication problem: Receiver did not receive data.	The Wave Receiver received a new RSP_UD.
5	b_5	Clock synchronization error	- The received timestamp deviates from the current date & time more than 60s (set by ACM WAVE TRANSMITTER).	The clock has been synchronized successfully.
			- The received timestamp is equal or less than the date time value of the last transmission. (set by Absolute Encoder AE2)	A new user key is set.
6	b_6	Fraud attempt	- Encryption verification failed (see 4.1.3)	A new user key is set.
7	b_7	Valve alarm	- received command “release valve” - a valve command was not executed successfully - the valve voltage is not ok	A new user key is set.

Table 17: Error Status Codes

4.3.5 Version

The Version field is implemented as a bit mask:

b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0
Protocol Type		Protocol Version					

Table 18: Version Field

Protocol Type

Code	Meaning
00	Elster M-Bus
01	Elster P2
10	Elster OMS
11	Reserved for future use

Table 19: Protocol Type Definitions

The Protocol Version represents the version of the Protocol, e.g. P2 v2.2.

Protocol Version for Protocol Type = 'Elster P2'

Code	Meaning
000000	P2 v2.2 Elster Implementation (this document)
any other value	Reserved for future P2 Implementations

Table 20: Protocol Version Definition

4.4 Variable Data Blocks

4.4.1 Data Points Overview

ID	Name	Data Record Header				
		DIF	DIFE	VIF	VIFE	LVAR
D001	User Key LSB	07	-	FD	19	-
D002	User Key MSB Storage Bit = 0	07	-	FD	19	-
D003	User Key MSB Storage Bit = 1	47	-	FD	19	-
D004	Serial number	0D	-	78	-	11
D005	Volume, converted	0C / 4C	-	13…14	-	-
D006	Volume, unconverted	0C / 4C	-	93…94	3A	-
D007	Valve Status	89	40	FD	1A	-
D008	Valve Control	01	-	FD	1F	-
D009	Meter Configuration Data	01	-	FD	67	-
D010	Meter Clock Time	06	-	6D	-	-
D011	Timestamp	46	-	6D	-	-
D012	Primary Address	01	-	7A	-	-

Table 21: Data Points

4.4.2 User Key LSB

	Field	Hex	Remark
0	DIF	07	64 bit data, Storage 0 => (64 LSB bits of encryption key)
1	VIF	FD	VIF from table 11
2	VIFE	19	Reserved -> AES 128 KEY exchange
3	User Key 1	AES-0	AES-0 -> AES-7, where AES-0 is the LSB in the LSB half of the key.
4	User Key 2	AES-1	
5	User Key 3	AES-2	
6	User Key 4	AES-3	
7	User Key 5	AES-4	
8	User Key 6	AES-5	
9	User Key 7	AES-6	
10	User Key 8	AES-7	

Data Point D001 User Key LSB

4.4.3 User Key MSB Storage Bit = 0

	Field	Hex	Remark
0	DIF	07	64 bit data, Storage 0 => (64 MSB bits of encryption key)
1	VIF	FD	VIF from table 11
2	VIFE	19	Reserved -> AES 128 KEY exchange
3	User Key 9	AES-8	AES-8 -> AES-15, where AES-8 is the LSB in the MSB half of the key.
4	User Key 10	AES-9	
5	User Key 11	AES-10	
6	User Key 12	AES-11	
7	User Key 13	AES-12	
8	User Key 14	AES-13	
9	User Key 15	AES-14	
10	User Key 16	AES-15	

Data Point D002: User Key MSB Storage Bit = 0

Note 1: For compatibility reasons, the MSB half of the key shall be coded with DIF = 07h, i.e. the Storage Number Bit is set to 0 for both parts of the key.

4.4.4 User Key MSB Storage Bit = 1

	Field	Hex	Remark
0	DIF	47	64 bit data, Storage 1 => (64 MSB bits of encryption key)
1	VIF	FD	VIF from table 11
2	VIFE	19	Reserved -> AES 128 KEY exchange
3	User Key 9	AES-8	AES-8 -> AES-15, where AES-8 is the LSB in the MSB half of the key.
4	User Key 10	AES-9	
5	User Key 11	AES-10	
6	User Key 12	AES-11	
7	User Key 13	AES-12	
8	User Key 14	AES-13	
9	User Key 15	AES-14	
10	User Key 16	AES-15	

Data Point D003: User Key MSB Storage Bit = 1

4.4.5 Serial number

	Field		Hex	Remark
0	DIF		0D	Variable Length ASCII
1	VIF		78	Equipment Identifier
2	LVAR		11	Length = 17
3	Equipment Identifier	Year of manufacturing	EI-0	2 characters, ASCII coded LSB (i.e. last character) first
4			EI-1	
5		Serial number	EI-2	10 characters, ASCII coded LSB (i.e. last character) first.
6			EI-3	
7			EI-4	
8			EI-5	
9			EI-6	
10			EI-7	
11			EI-8	
12			EI-9	
13			EI-10	
14			EI-11	
15		KIWA-Gastec label	EI-12	5 characters, ASCII coded LSB (i.e. last character) first.
16			EI-13	
17			EI-14	
18			EI-15	
19			EI-16	

Data Point D004: Serial number

Note 1: If the KIWA-Gastec label is shorter than 5 characters, leading spaces (coded as 20h) shall be added.

Note 2: If the serial number is shorter than 10 characters, leading zeroes (coded as 30h) shall be added.

4.4.6 Volume, converted

	Field	Hex	Remark
0	DIF	0C / 4C	Data format 8 Digit BCD, Storage Number Bit = 0 / 1
1	VIF	13…14	Multiplier 0,001 m³ ...0,01 m³
2	Volume	V-0	Temperature Converted Value, where V0 is the LSB of the value
3		V-1	
4		V-2	
5		V-3	

Data Point D005: Volume, converted

Note 1: Storage Number Bit = 1 signifies time stamped value with respect to current time stamp (see also 4.4.12).

4.4.7 Volume, unconverted

	Field	Hex	Remark
0	DIF	0C / 4C	Data format 8 Digit BCD, Storage Bit = 0 / 1
1	VIF	93…94	Multiplier 0,001 m³ ... 0,01 m³
2	VIFE	3A	VIF contains unconverted units.
3	Volume	V-0	Unconverted volume where V0 is the LSB of the value
4		V-1	
5		V-2	
6		V-3	

Data Point D006: Volume, unconverted

Note 1: Storage Number Bit = 1 signifies time stamped value with respect to current time stamp (see also 4.4.12).

4.4.8 Valve Status

	Field	Hex	Remark
0	DIF	89	2 digit BCD
1	DIFE	40	Subunit
2	VIF	FD	Valve (new definition)
3	VIFE	1A	Digital Status
4	Valve Status	00…01	00: valve closed 01: valve opened

Data Point D007: Valve Status

4.4.9 Valve Control

	Field	Hex	Remark
5	DIF	01	2 digit BCD
6	VIF	FD	Valve (new definition)
7	VIFE	1F	Remote Control
8	Valve Status	00…01	00: close the valve 01: open the valve

Data Point D008: Valve Control

Note 1: The Valve Command “release” (code = 02h) is not used. If the slave receives this command, the error status code “Valve Alarm” shall be set (see 4.3.4).

4.4.10 Meter Configuration Data

	Field	Hex	Remark
0	DIF	01	1 digit binary
1	VIF	FD	Extension
2	VIFE	67	Special Supplier Information
3	Meter Configuration	MM	Meter Configuration Mask

Data Point D009: Meter Configuration Data

Meter Configuration Mask:

$b_7\ b_6\ b_5\ b_4\ b_3\ b_2\ b_1\ b_0$

	Bit	Meaning with Bit set	Significance with bit not set
0	b_0	Clock Device Implemented	No clock device implemented
1	b_1	Switching Device (Valve) Implemented	No switching device implemented
2	b_2	Meter provides temperature converted volume	Meter provides unconverted volume
3	b_3	n.a.	n.a.
4	b_4	n.a.	n.a.
5	b_5	n.a.	n.a.
6	b_6	n.a.	n.a.
7	b_7	n.a.	n.a.

Table 22: Meter Configuration Mask

4.4.11 Meter Clock Time

	Field	Hex	Remark
0	DIF	06	6 Bytes Integer
1	VIF	6D	Extended Date and Time compound data type I
2	Meter Clock Time	T-0	current meter clock time
3		T-1	
4		T-2	
5		T-3	
6		T-4	
7		T-5	

Data Point D010: Meter Clock Time

Note 1: The date time value shall be in UTC.

4.4.12 Timestamp

This data record is used to provide a timestamp to an index value (see also 4.4.6 and 4.4.7).

	Field	Hex	Remark
0	DIF	46	6 Bytes Integer
1	VIF	6D	Extended Date and Time compound data type I
2	Meter Clock Time	T-0	current meter clock time
3		T-1	
4		T-2	
5		T-3	
6		T-4	
7		T-5	

Data Point D011: Timestamp

Note 1: The date time value shall be in UTC.

4.4.13 Primary Address

	Field	Hex	Remark
9	DIF	01	Data identifier
10	VIF	7A	Address data
11	Primary Addressing	A-0	New primary address

Data Point D012: Primary Address

4.5 Procedures

4.5.1 Overview

ID	Telegram Name	CI-Field
P001	SND_UD Set Primary Address	51
P002	SND_UD Set User Key	5A
P003	SND_UD Set Date And Time	5A
P004	SND_UD Valve Control	5A
P005	SND_UD Application Reset	50
P006	SND_UD Slave Select	52
P007	RSP_UD Standard Data Record	72

Table 23: Procedures Overview

4.5.2 SND_UD Set Primary Address

	Field	Hex		Remark
		clear	encrypted	
0	*SND_UD Frame*			
1	*Control Information: 51 Data send (master to slave)*			
2	*Data Point D012 Primary Address*			

Procedure P001: SND_UD Set Primary Address

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 2: M-bus devices (e.g. Encoder) 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.

Note 3: Dongle devices using transparent data transfer (e.g. ACM WAVE SYSTEM) shall only accept this telegram when their current primary address is zero. These Dongle Devices shall ignore this telegram when their current primary address is unequal to zero.

4.5.3 SND_UD Set User Key

	Field	Hex	Remark
3	*SND_UD Frame*		
4	*Control Information: 5A Data send (master to slave)*		
5	*Data Point D001 User Key LSB*		
6	*Data Point D002 User Key MSB Storage Bit = 0* *or* *Data Point D003User Key MSB Storage Bit = 1*		

Procedure P002: SND_UD Set User Key

Note 1: Setting the User Key to "00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00" means no User Key is defined, i.e. all subsequent communication is unencrypted.

Note 2: The User Key is encrypted with the Default Key, using AES-128 with an Initialization Vector set to:

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

4.5.4 SND_UD Set Date And Time

	Field
0	*SND_UD Frame*
1	*Control Information: 5A Data send (master to slave)*
2	*Short Data Header*
3	*Encryption Verification*
4	*Data Point D010* Meter Clock Time
5	*[Idle Filler]*

Procedure P003: SND_UD Set Date And Time

Note 1: Any command from Master to Slave sent with Encryption Method 4 sets the clock of the Slave, since the first field is a date time value.

Note 2: Deviation of more than 60 s is reported by bit 5 in the Status field (see also chapter 4.3.4).

Note 3: The master sends this command to the slave only if the bit 'Clock Device Implemented' is set in the data point 'Meter Configuration Data' (see also chapter 4.4.10).

4.5.5 SND_UD Valve Control

	Field
6	*SND_UD Frame*
7	*Control Information: 5A Data send (master to slave)*
8	*Short Data Header*
9	*Encryption Verification*
10	*Data Point D008* Valve Control
11	*[Idle Filler]*

Procedure P004: SND_UD Valve Control

Note 4: Sending a valve command with Encryption Method 4 will also set the date and time, since the first element will be a set date and time field.

Note 5: The master sends this command to the slave only if the bit 'Switching Device Implemented' is set in the data point 'Meter Configuration Data' (see also chapter 4.4.10).

4.5.6 SND_UD Application Reset

	Field
0	*SND_UD Frame*
1	*Control Information: 50 Application Reset*

Procedure P005: SND_UD Application Reset

4.5.7 SND_UD Slave Select

	Field
0	*SND_UD Frame*
1	*Control Information: 52 Slave Select*
2	*Short ID*

Procedure P006: SND_UD Slave Select

4.5.8 RSP_UD Standard Data Record

	Field
0	*RSP_UD Frame*
1	*Control Information: 72 slave to master*
2	*Fixed Data Header*
3	*Encryption Verification*
4	*Data Point D004 Serial number*
5	*Data Point D005 Volume, converted* *or* *Data Point D006Volume, unconverted*
6	*[Data Point D011 Timestamp]*
7	*[Data Point D007 Valve Status]*
8	*Data Point D009 Meter Configuration Data*

Procedure P007: RSP_UD Standard Data Record

Note 1: If the signature field is set to “00 00” (i.e. no encryption is used), the encryption verification field is missing.

Note 2: In connection ACM WIRED M-BUS, the data point D011 *Timestamp* is missing.

Note 3: If the meter has no valve, the data point D007 *Valve Status* is missing.

y

5 Abbreviation list

n.a. not applicable

6 References

[1] EN 13757-3:2004
Communication Systems for and remote reading of meters –
Part 3: Dedicated application layer

[2] EN 60870-5-2:1993
Telecontrol equipment and systems –
Part 5: Transmission Protocols
Section 2: Link Transmission Procedures

[3] P2 Companion Standard – Dutch Smart Meter Requirements
April 18th, 2008; Version 2.2

Appendix

Annex A Protocol Implementation Conformance Statement

A.1 Supported C-Fields

C-Field Name	AE2	ACM WAVE TRANSMITTER	ACM WAVE RECEIVER
SND_NKE	Yes	Yes	Yes
REQ_UD1	Yes	Yes	Yes
REQ_UD2	Yes	Yes	Yes
SND_UD	Yes	Yes	Yes
RSP_UD	Yes	Yes	Yes

Table 24: Supported C-Fields

A.2 Supported CI-Fields

Control Information	AE2	ACM WAVE TRANSMITTER	ACM WAVE RECEIVER
Application Reset	Yes	Yes	Yes
Command to device	Yes	Yes	Yes
Selection of device	Yes	Yes	Yes
Command to device, Short Data Header	Yes	Yes	Yes
Command to device, Long Data Header	Yes	Yes	Yes
Response from device, Fixed Data Header	Yes	Yes	Yes

Table 25: Supported CI-Fields

A.3 Supported Data Points

Data Point Name	AE2	ACM WAVE TRANSMITTER	ACM WAVE RECEIVER
D001: User Key LSB	Yes	Yes	Yes
D002: User Key MSB Storage Bit = 0	C1	Yes	Yes
D003: User Key MSB Storage Bit = 1	C1	Yes	Yes
D004: Serial number	Yes	Yes	Yes
D005: Volume, converted	C2	Yes	Yes
D006: Volume, unconverted	C2	Yes	Yes
D007: Valve Status	C4	C4	C4
D008: Valve Control	Yes	Yes	Yes
D009: Meter Configuration Data	Yes	Yes	Yes
D010: Meter Clock Time	C3	Yes	Yes
D011: Timestamp	C3	Yes	Yes
D012: Primary Address	yes	Yes	Yes

Table 26: Supported Data Points

Condition C1: Depending on parameterization
Condition C2: Depending on parameterization
Condition C3: Only if ACM WAVE SYSTEM is connected
Condition C4: If the meter contains a valve.

A.4 Supported Procedures

ID	Telegram Name	AE2	ACM WAVE TRANSMITTER	ACM WAVE RECEIVER
P001: SND_UD Set Primary Address		Yes	Yes	Yes
P002: SND_UD Set User Key		Yes	Yes	Yes
P003: SND_UD Set Date And Time		Yes	Yes	Yes
P004: SND_UD Valve Control		Yes	Yes	Yes
P005: SND_UD Application Reset		Yes	Yes	Yes
P006: SND_UD Slave Select		Yes	Yes	Yes
P007: RSP_UD Standard Data Record		Yes	Yes	Yes

Table 27: Supported Procedures

Annex B Examples

B.1 SND_NKE

	Field	Hex	Remark
5	Start Character	10	Sort frame
6	C-Field	40	SND_NKE
7	Primary Address	01	e.g. 01
8	Checksum	41	
9	Stop Character	16	

Example 2: SND_NKE

B.2 REQ_UD1

	Field	Hex	Remark
5	Start Character	10	Start byte sort telegram
6	C	5A	Request User Data (counter sending) FCB=0
7	A	01	Primary Address
8	CS	5B	Checksum
9	Stop Character	16	Always 16

Example 3: REQ_UD1

B.3 REQ_UD2

	Field	Hex	Remark
5	Start Character	10	Start byte sort telegram
6	C	5B	Request User Data (counter sending) FCB=0
7	A	01	Primary Address
8	CS	5C	Checksum
9	Stop Character	16	Always 16

Example 4: REQ_UD2

B.4 SND_UD Set primary address

	Field	Hex		Remark
		clear	encrypted	
0	Start Character	68		Start byte long telegram
1	L	06		Length
2	L	06		Length
3	Start Character	68		Start byte long telegram
4	C	53		(FCB=0)
5	A	01		Primary Address
6	CI	51		Data send (master to slave)
7	DIF	01		Data identifier
8	VIF	7A		Address data
9	Primary Addressing	02		New primary address
10	CS	22		Checksum
11	Stop Character	16		Always 16

Example 5: Change primary address from 01 to 02

B.5 SND_UD Set User Key

The User Key is encrypted with the Default Key (see chapter 1.1):

```
27 9F B7 4A 75 72 13 5E 8F 9B 8E F6 D1 EE E0 03
```

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
0	Start Character	68	Start byte long telegram
1	L	19	Length
2	L	19	Length
3	Start Character	68	Start byte long telegram
4	C	53	(FCB=0)
5	A	01	Primary Address
6	CI	51	Data send (master to slave)
7	DIF	07	64 bit data, Storage 0
8	VIF	FD	VIF from table 11
9	VIFE	19	Reserved -> AES 128 KEY exchange
10	User Key 1	03	Block containing the LSB (LSB first)
11	User Key 2	E0	
12	User Key 3	EE	
13	User Key 4	D1	
14	User Key 5	F6	
15	User Key 6	8E	
16	User Key 7	9B	
17	User Key 8	8F	
18	DIF	07	64 bit data, Storage 0
19	VIF	FD	VIF from table 11
20	VIFE	19	Reserved -> AES 128 KEY exchange
21	User Key 9	5E	Block containing the MSB (LSB first)
22	User Key 10	13	
23	User Key 11	72	
24	User Key 12	75	
25	User Key 13	4A	
26	User Key 14	B7	
27	User Key 15	9F	
28	User Key 16	27	
29	CS	4E	Checksum
30	Stop Character	16	Always 16

Example 6: Key Exchange

B.6 SND_UD Set Date and Time

	Field	Hex		Remark
		clear	encrypted[1]	
0	Start Character	68		Start byte long telegram
1	L	17		Length
2	L	17		Length
3	Start Character	68		Start byte long telegram
4	C	53		FCB=0
5	A	01		Address = 01
6	CI	5A		Data send (master to slave)
7	Access No	01		
8	Status	00		
9	Signature	00	10	AES 128, Mode 4 16 bytes encrypted
10		00	04	
11	DIF	06	C0	6 Bytes Integer / Binary
12	VIF	6D	F9	Extended Date and Time compound data type I
13	Date & Time	00	F4	May 28th, 2009; 08:14:00, Day of week = 0 Week = 0 Time = valid Daylight saving, leap year as required
14		0E	FC	
15		08	23	
16		3C	C5	
17		15	3B	
18		00	B2	
19	Filler	2F	61	Idle Filler
20		2F	80	
21		2F	C4	
22		2F	C8	
23		2F	43	
24		2F	70	
25		2F	3D	
26		2F	E1	
27	CS	01	7F	Checksum
28	Stop Character	16		Always 16

Example 7: Set Date and Time, Encryption Method Code = 04h

Note 1: Encryption Method Code 05h is not applicable for this command.

[1] The User Key is defined in chapter 1.1.

B.7 SND_UD Valve Control

B.7.1 Close the valve

Encryption Method Code = 04h

	Field	Hex		Remark
		clear	encrypted[2]	
0	Start Character	68		Start byte long telegram
1	L	17		Length
2	L	17		Length
3	Start Character	68		Start byte long telegram
4	C	53		FCB=0
5	A	01		Primary Address
6	CI	5A		Data send (master to slave)
7	Access No	01		
8	Status	00		
9	Signature	00	10	AES 128, Mode 4 16 bytes encrypted
10		00	04	
11	DIF	06	F3	6 Bytes Integer / Binary
12	VIF	6D	28	Extended Date and Time compound data type I
13	Date &Time	00	7C	May 28th, 2009; 08:14:00, Day of week = 0 Week = 0 Time = valid Daylight saving, leap year as required
14		0E	97	
15		08	C1	
16		3C	97	
17		15	7E	
18		00	FF	
19	DIF	01	AB	8 bit Integer / Binary
20	VIF	FD	47	Extension
21	VIFE	1F	3B	Remote Control
22	Valve Command	00	5C	Command = close
23	Filler	2F	4A	Idle Filler
24		2F	3D	
25		2F	57	
26		2F	47	
27	CS	62	74	Checksum
28	Stop Character	16		Always 16

Example 8: Valve Control Command = 'close', Encryption Method Code = 04h

[2] The User Key is defined in chapter 1.1.

Encryption Method Code = 05h

	Field	Hex		Remark
		clear	encrypted[3]	
0	Start Character	68		Start byte long telegram
1	L	17		Length
2	L	17		Length
3	Start Character	68		Start byte long telegram
4	C	53		FCB=0
5	A	01		Primary Address
6	CI	5A		Data send (master to slave)
7	Access No	01		
8	Status	00		
9	Signature	00	10	AES 128, Mode 5
10		00	05	16 bytes encrypted
11	Encryption Verification	2F	C3	Encryption Verification
12		2F	03	
13	DIF	01	C3	8 bit Integer / Binary
14	VIF	FD	3B	Extension
15	VIFE	1F	CB	Remote Control
16	Valve Command	00	AB	Command = close
17	Filler	2F	ED	Idle Filler
18		2F	51	
19		2F	2D	
20		2F	24	
21		2F	BD	
22		2F	B6	
23		2F	88	
24		2F	F1	
25		2F	3E	
26		2F	3F	
27	CS	00	F6	Checksum
28	Stop Character	16		Always 16

Example 9: Valve Control Command = ‘close’, Encryption Method Code = 05h

[3] The User Key and the Initialization Vector are defined in chapter 1.1.

B.7.2 Open the valve

Encryption Method Code = 04h

	Field	Hex		Remark
		clear	encrypted[4]	
0	Start Character	68		Start byte long telegram
1	L	17		Length
2	L	17		Length
3	Start Character	68		Start byte long telegram
4	C	53		FCB=0
5	A	01		Primary Address
6	CI	5A		Data send (master to slave)
7	Access No	01		
8	Status	00		
9	Signature	00	10	AES 128, Mode 4 16 bytes encrypted
10		00	04	
11	DIF	06	34	6 Bytes Integer / Binary
12	VIF	6D	95	Extended Date and Time compound data type I
13	Date &Time	00	2F	May 28th, 2009; 08:14:00, Day of week = 0 Week = 0 Time = valid Daylight saving, leap year as required
14		0E	07	
15		08	20	
16		3C	1B	
17		15	AA	
18		00	2C	
19	DIF	01	94	8 bit Integer / Binary
20	VIF	FD	DA	Extension
21	VIFE	1F	98	Remote Control
22	Valve Command	01	D8	Command = open
23	Filler	2F	12	Idle Filler
24		2F	26	
25		2F	F9	
26		2F	E6	
27	CS	63	C8	Checksum
28	Stop Character	16		Always 16

Example 10: Valve Control Command = ‘open’, Encryption Method Code = 04h

[4] The User Key is defined in chapter 1.1.

Encryption Method Code = 05h

	Field	Hex		Remark
		clear	encrypted[5]	
0	Start Character	68		Start byte long telegram
1	L	17		Length
2	L	17		Length
3	Start Character	68		Start byte long telegram
4	C	53		FCB=0
5	A	01		Primary Address
6	CI	5A		Data send (master to slave)
7	Access No	01		
8	Status	00		
9	Signature	00	10	AES 128, Mode 5 16 bytes encrypted
10		00	05	
11	Encryption Verification	2F	20	Encryption Verification
12		2F	15	
13	DIF	01	DD	8 bit Integer / Binary
14	VIF	FD	5E	Extension
15	VIFE	1F	9E	Remote Control
16	Valve Command	01	9C	Command = open
17	Filler	2F	95	Idle Filler
18		2F	1D	
19		2F	FA	
20		2F	C9	
21		2F	F7	
22		2F	F5	
23		2F	E2	
24		2F	06	
25		2F	D5	
26		2F	BB	
27	CS	01	47	Checksum
28	Stop Character	16		Always 16

Example 11: Valve Control Command = ‘open’, Encryption Method Code = 05h

[5] The User Key and the Initialization Vector are defined in chapter 1.1.

B.8 SND_UD Application Reset

	Field	Hex		Remark
		clear	encrypted	
0	Start Character	68		Start byte long telegram
1	L	03		Length
2	L	03		Length
3	Start Character	68		Start byte long telegram
4	C	53		FCB=0
5	A	01		Primary Address
6	CI	50		Application Reset
7	CS	A4		Checksum
8	Stop Character	16		Always 16

Example 12: Application Reset

B.9 SND_UD Slave Select

	Field	Hex		Remark
		clear	encrypted	
0	Start Character	68		Start byte long telegram
1	L	0B		Length
2	L	0B		Length
3	Start Character	68		Start byte long telegram
4	C	53		FCB=0
5	A	FD		Secondary Addressing
6	CI	52		Slave Select
7	Identification Number	78		Identification Number, e.g. 12345678
8		56		
9		34		
10		12		
11	Manufacturer ID	93		Manufacturer ID e.g. “ELS”
12		15		
13	Version	33		
14	Medium	03		
15	CS	94		Checksum
16	Stop Character	16		Always 16

Example 13: Slave Select

B.10 Standard Data Record ACM M-BUS WIRE

Example 14 shows a RSP_UD telegram of a meter comprising of the following properties:

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

	Field	Hex		Remark
		clear	encrypted[6]	
0	Start Character	68		Start byte long telegram
1	L	3F		Length
2	L	3F		Length
3	Start Character	68		Start byte long telegram
4	C	08		(FCB=0)
5	A	01		Primary Address
6	CI	72		Data send (master to slave)
7	Identification Number	78		Identification Number, e.g. 12345678
8		56		
9		34		
10		12		
11	Manufacturer ID	93		Manufacturer ID, e.g. “ELS”
12		15		
13	Generation	33		Version = 51
14	Medium	03		Medium = gas
15	Access No	01		Access Number = 01
16	Status	82		Error Status: - Any Application Error - Valve Alarm
17	Signature	00	30	AES 128, Method 5 48 Bytes encrypted
18		00	05	
19	Encryption Verification	2F	C3	Encryption Verification
20		2F	B0	
21	DIF	0D	EF	Equipment Identifier 17 Bytes, ASCII coded “ABCD1234567891234”
22	VIF	78	DF	
23	LVAR	11	1F	
24	Data	34	B7	
25		33	46	
26		32	A6	
27		31	75	
28		39	DA	
29		38	0F	
30		37	3D	
31		36	98	

[6] The User Key and the Initialization Vector are defined in chapter 1.1.

	Field	Hex		Remark
		clear	encrypted[6]	
32		35	EC	
33		34	1C	
34		33	DD	
35		32	85	
36		31	D6	
37		44	0B	
38		43	33	
39		42	29	
40		41	2C	
41	DIF	0C	5B	Temperature Converted Volume Multiplier = 0,001 m³ Value = 1,230 m³
42	VIF	13	B1	
43	Data	30	30	
44		12	31	
45		00	BD	
46		00	2A	
47	DIF	89	FD	Valve Status = opened
48	DIFE	40	DA	
49	VIF	FD	66	
50	VIFE	1A	0B	
51	Data	01	78	
52	DIF	01	D5	Meter Configuration Data - no clock device implemented - Valve implemented - Meter provides temperature converted volume
53	VIF	FD	21	
54	VIFE	67	E3	
55	Data	06	34	
56	Idle Filler	2F	CC	Idle Filler
57		2F	DD	
58		2F	6C	
59		2F	B4	
60		2F	66	
61		2F	FD	
62		2F	AF	
63		2F	26	
64		2F	9B	
65		2F	88	
66		2F	08	
67	CS	47	7B	Checksum
68	Stop Character	16		16

Example 14: RSP_UD telegram of an Elster Gas Meter with wired M-Bus

Note 2: If the signature field is set to “00 00” (i.e. no encryption is used), the encryption verification field is missing.

B.11 Standard Data Record ACM WAVE SYSTEM RF

Example 15 shows a RSP_UD telegram of a meter comprising of the following properties:

- with valve
- unconverted volume
- meter family G10 => volume multiplier = 0,01m³

	Field	Hex clear	Hex encrypted[7]	Remark
0	Start Character	68		Start byte long telegram
1	L	4F		Length
2	L	4F		Length
3	Start Character	68		Start byte long telegram
4	C	08		(FCB=0)
5	A	01		Primary Address
6	CI	72		Data send (master to slave)
7	Identification Number	78		Identification Number, e.g. 12345678
8		56		
9		34		
10		12		
11	Manufacturer ID	93		Manufacturer ID, e.g. “ELS”
12		15		
13	Generation	33		Version = 51
14	Medium	03		Medium = gas
15	Access No	01		Access Number = 01
16	Status	04		Error Status: - Low Power
17	Signature	00	40	AES 128, Method 4 64 Bytes encrypted
18		00	04	
19	Encryption Verification	06	94	Encryption Verification Date/Time May 28th, 2009, 08:14:00
20		6D	BF	
21		00	08	
22		0E	C7	
23		08	65	
24		3C	83	
25		15	FE	
26		00	E0	
27	DIF	0D	06	Variable Length ASCII
28	VIF	78	CD	Equipment Identifier
29	LVAR	11	69	Length = 17
30	Equi Year of	39	2F	e.g. “09”
31	manufacturing	30	F8	

[7] The User Key and the Initialization Vector are defined in chapter 1.1.

	Field		Hex		Remark
			clear	encrypted[7]	
32		Serial number	38	7C	e.g. “0012345678” (see also lines 7 – 10)
33			37	A7	
34			36	21	
35			35	1E	
36			34	FD	
37			33	30	
38			32	03	
39			31	5A	
40			30	60	
41			30	0B	
42		KIWA-Gastec label	5A	28	e.g. “00XYZ”
43			59	A6	
44			58	38	
45			30	D9	
46			30	A5	
47	DIF		46	E4	Timestamp May 28th, 2009, 08:14:00 Day of week = 0 Week = 0 Time = valid
48	VIF		6D	EC	
49	Data		00	08	
50			0E	C3	
51			08	F5	
52			3C	F6	
53			15	4C	
54			00	16	
55	DIF		4C	BC	Unconverted Volume Multiplier = 0,01 m³ Value = 12,30 m³
56	VIF		94	C8	
57	VIFE		3A	6C	
58	Data		30	5E	
59			12	CC	
60			00	88	
61			00	73	
62	DIF		89	F9	Valve Status = opened
63	DIFE		40	B9	
64	VIF		FD	8C	
65	VIFE		1A	D8	
66	Data		00	36	
67	DIF		01	E9	Meter Configuration Data - clock device implemented - Valve implemented - Meter provides unconverted volume
68	VIF		FD	43	
69	VIFE		67	A0	
70	Data		03	BE	
71	Idle Filler		2F	F3	Idle Filler

	Field	Hex		Remark
		clear	encrypted[7]	
72		2F	86	
73		2F	01	
74		2F	51	
75		2F	C5	
76		2F	BF	
77		2F	CC	
78		2F	CF	
79		2F	04	
80		2F	21	
81		2F	9D	
82		2F	CB	
83	Checksum	B0	1C	Checksum
84	Stop Character	16		

Example 15: RSP_UD telegram of an Elster Gas Meter with ACM WAVE SYSTEM RF