Open Metering System Specification

Message examples

Annex N to
Volume 2 Primary Communication
Issue 4.3.3

RELEASE D (2020-10-22)

Document History

Version	Date	Comment	Editor
A 0.1.0	2013-09-28	Import from OMS-Spec. Vol.2 Issue 3.0.1 Add new example Fragmentation	Uwe Pahl
A 0.2.0	2013-10-22	Insert updated examples	Uwe Pahl
A 0.3.0	2014-01-16	Editorial Review- see enquiry comments	Uwe Pahl
A 0.3.1	2014-01-17	Add ACC-NR	Uwe Pahl
A 0.3.2	2014-01-25	Update HCA - N.3.3 und N.3.4 Release A	Uwe Pahl
B 0.4.0	2016-01-22	Editorial updates Change Serial No → Ident No Add M-Bus Example for Encryption mode B	Thomas Banz
B 0.4.1	2016-10-21	Editorial review -> Release candidate	Thomas Banz, Uwe Pahl
B 0.4.2	2016-12-16	Release B	Achim Reissinger, Alexander Rohleder, Uwe Pahl, Thomas, Banz
C 0.4.2	2019-10-28	Add overview tables, Update examples (ELL), Bugfixes	Achim Reisinger. Alexander Rohleder, Thomas Banz
C 0.4.3	2020-01-08	Reference on page 4 corrected	Achim Reissinger
D 0.4.4	2020-06-03	Chapters N.10.1 to N.10.3 added	Achim Reissinger, Thomas Banz, Thomas Blank, Dirk Matussek, Uwe Pahl
D 0.4.5	2020-06-04	N.10.3 headline and content changed Editorial changes in N.10.1 and N.10.2	Achim Reissinger, Thomas Banz
D 0.4.6	2020-06-04	Editorial changes	Achim Reissinger, Uwe Pahl
D 0.4.7	2020-06-05	Editorial change	Achim Reissinger, Thomas Banz
D 0.4.8	2020-07-07 and 2020-07-09	Updated title page Editorial changes	Achim Reissinger
D 1.0.0	2020-09-24	Release candidate	Achim Reissinger
D 1.0.1	2020-09-29	Update N.7 acc. to Annex M UC-04	Uwe Pahl
D 1.0.2	2020-10-16	Changes during meeting #106	Thomas Blank, Uwe Pahl, Achim Reissinger
D 1.0.3	2020-10-19	Release	Achim Reissinger

Contents

N.1 Overview Tables

Wireless examples:

Message Type	Security Profile	Chapter
SND-NR	A	N.2.1
SND-NR	B	N.2.3
REQ-UD2/RSP-UD	B	N.2.4
REQ-UD2/RSP-UD (fragmented)	B	N.3
ACC-NR	No	N.5.2
SND-NR (partial encrypted)	A	N.5.3
SND-IR/CNF-IR	A	N.6
SND-UD/ACK	A	N.7
RSP-UD	A	N.8
RSP-UD (APL-error)	No	N.8
ACC-DMD/ACK	No	N.9
SND-NKE	No	N.10
SND-NR (wM-Bus)	B+ASP10	N.11.1
SND-UD2 (wM-Bus)	B+ASP10	N.11.2
RSP-UD (wM-Bus Set Breaker - successful)	B+ASP10	N.11.3
RSP-UD (wM-Bus Set Breaker - failure)	B+ASP10	N.11.4

Wired examples:

Message Type	Security Profile	Chapter
RSP-UD	No	N.2.2
RSP-UD	B	N.2.5
REQ-UD2/RSP-UD (fragmented)	A	N.4
RSP_UD (partial encrypted)	A	N.5.4

N.2 Gas Meter with different Security profiles

N.2.1. wM-Bus Meter with Security profile A

This example shows a synchronous transmission of wM-Bus Meter with integrated radio interface (short TPL) using Security Profile A.

5

Gas meter example	
Medium	Gas
Manufacturer	ELS
Ident number	12345678
Version	51
Forward absolute meter volume, temperature converted	28504,27 m³
date and time of read out	31.05.2008 23:50
Error code binary	0

AES Key according to FIPS 197 (see 9.1):
= manu. spec. at least 8 bytes unique for each meter
= 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 11

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

SND-NR (wM-Bus)

		OMS wM-Bus frame	Gas meter example		Layer
Byte No	Field Name	Content	Bytes [hex] plain	Bytes [hex] AES coded	
1	L Field	Length of data (46 bytes)		2Eh	Data Link Layer (DLL)
2	C Field	Send - No Reply		44h	
3	M Field	Manufacturer code		93h	
4	M Field	Manufacturer code		15h	
5	A Field	Ident No LSB (BCD)		78h	
6	A Field	Ident No (BCD)		56h	
7	A Field	Ident No (BCD) (= 12345678)		34h	
8	A Field	Ident No MSB (BCD)		12h	
9	A Field	Version (or Generation number)		33h	
10	A Field	Device type (Medium=Gas)		03h	
11	CRC 1			33h	
12	CRC 1			63h	
13	CI Field	7Ah (short header)		7Ah	Transport Layer (TPL)
14	Access No.	Shared Access number of Meter		2Ah	
15	Status	M-Bus state contents errors and alerts		00h	
16	Config Field	NNNNCCRHb (2 encr. blocks)		20h	
17	Config Field	BASMMMMMb (unidir., sync., AES)		25h	

18	AES-Verify	Encryption verification	2Fh	59h		TPL
19	AES-Verify	Encryption verification	2Fh	23h		
20	DR1	DIF (8 digit BCD)	0Ch	C9h	# 1	Application Layer (APL)
21	DR1	VIF (Volume 0,01 m³)	14h	5Ah		
22	DR1	Value LSB	27h	AAh		
23	DR1	Value	04h	26h		
24	DR1	Value (= 28504,27 m³)	85h	D1h		
25	DR1	Value MSB	02h	B2h		
26	DR2	DIF (Time at readout; Type F)	04h	E7h		
27	DR2	VIF (Date, Time)	6Dh	49h		
28	DR2	Value LSB	32h	3Bh		
29	CRC 2			C2h	DLL	
30	CRC 2			ADh		
31	DR2	Value	37h	01h	# 1	APL
32	DR2	Value (31.05.2008 23:50)	1Fh	3Eh		
33	DR2	Value MSB	15h	C4h		
34	DR3	DIF (2 byte integer)	02h	A6h		
35	DR3	VIF (VIF-Extension Table FD)	FDh	F6h		
36	DR3	VIFE (error flag)	17h	D3h	# 2	
37	DR3	Value LSB	00h	52h		
38	DR3	Value MSB (= 0)	00h	9Bh		
39	Dummy	Fill Byte due to AES	2Fh	52h		
40	Dummy	Fill Byte due to AES	2Fh	0Eh		
41	Dummy	Fill Byte due to AES	2Fh	DFh		
42	Dummy	Fill Byte due to AES	2Fh	F0h		
43	Dummy	Fill Byte due to AES	2Fh	EAh		
44	Dummy	Fill Byte due to AES	2Fh	6Dh		
45	Dummy	Fill Byte due to AES	2Fh	EFh		
46	Dummy	Fill Byte due to AES	2Fh	C9h		
47	CRC 3			55h	DLL	
48	CRC 3			B2h		
49	Dummy	Fill Byte due to AES	2Fh	9Dh	# 2	APL
50	Dummy	Fill Byte due to AES	2Fh	6Dh		
51	Dummy	Fill Byte due to AES	2Fh	69h		
52	Dummy	Fill Byte due to AES	2Fh	EBh		
53	Dummy	Fill Byte due to AES	2Fh	F3h		
54	CRC 4			ECh	DLL	
55	CRC 4			8Ah		

N.2.2. M-Bus Meter with no encryption:

This is an example of a RSP-UD after a REQ-UD2 (Meter ID and data are identical to wM-Bus Meter with Security profile A).

RSP-UD (M-Bus)

Byte No		OMS M-Bus frame	Gas meter example	Layer
	Field Name	Content	Bytes [hex]	
			plain	
1	Start	Start byte	68h	Data Link Layer (DLL)
2	L Field	Length of data (32 bytes)	20h	
3	L Field	Length of data (32 bytes)	20h	
4	Start	Start byte	68h	
5	C Field	Respond user data	08h	
6	A-Field	Secondary addressing mode	FDh	
7	CI Field	72h (long header)	72h	Transport Layer (TPL)
8	Ident.Nr.	Ident No LSB (BCD)	78h	
9	Ident.Nr.	Ident No (BCD)	56h	
10	Ident.Nr.	Ident No (BCD) (=12345678)	34h	
11	Ident.Nr.	Ident No MSB (BCD)	12h	
12	Manufr	Manufacturer code	93h	
13	Manufr	Manufacturer code	15h	
14	Version	Version (or Generation number)	33h	
15	Device type	Device type (Medium=Gas)	03h	
16	Access No.	Access number of Meter	2Ah	
17	Status	M-Bus state contents errors and alerts	00h	
18	Config Field	0000CCRHb	00h	
19	Config Field	BASMMMMMb	00h	
20	DR1	DIF (8 digit BCD)	0Ch	Application Layer (APL)
21	DR1	VIF (Volume 0,01 m³)	14h	
22	DR1	Value LSB	27h	
23	DR1	Value	04h	
24	DR1	Value (= 28504,27 m³)	85h	
25	DR1	Value MSB	02h	
26	DR2	DIF (Time at readout; Type F)	04h	
27	DR2	VIF (Date, Time)	6Dh	
28	DR2	Value LSB	32h	
29	DR2	Value	37h	
30	DR2	Value (31.05.2008 23:50)	1Fh	
31	DR2	Value MSB	15h	
32	DR3	DIF (2 byte integer)	02h	
33	DR3	VIF (FD-Table)	FDh	
34	DR3	VIFE (error flag)	17h	
35	DR3	Value LSB	00h	
36	DR3	Value MSB (= 0)	00h	
37	Checksum		89h	DLL
38	Stop	Stop byte	16h	

N.2.3. wM-Bus Meter with integrated radio and Security profile B

This example shows a synchronous transmission of a Gas Meter with an integrated unidirectional radio interface using security profile B.

Gas meter example	
Medium	Gas
Manufacturer	ELS
Ident number	12345678
Version	51
Forward absolute meter volume, temperature converted	28504,27 m³
Date and time of read out	31.05.2008 23:50
Error code binary	0

5

ToDo:
1. Calculate Session Keys
2. Encrypt Message using Kenc
3. Calculate MAC using Kmac
4. Calculate CRCs

Individual Master Key Mk (see 9.1):
=00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

Current Message Counter C (LSB first):
= B3 0A 00 00

Encryption Session Key Kenc
= CMAC(Mk, 0x00 || MCR || IdentNo || padding) = CMAC(Mk,00||B3||0A||00||00||78||56||34||12 … … ||07||07||07||07||07||07||07) = EC CF 39 D4 75 D7 30 B8 28 4F DF DC 19 95 D5 2F

MAC Session Key Kmac
= CMAC(Mk, 0x01 || MCR || IdentNo || padding) = CMAC(Mk,01||B3||0A||00||00||78||56||34||12 … … ||07||07||07||07||07||07||07) = C9 CD 19 FF 5A 9A AD 5A 6B BD A1 3B D2 C4 C7 AD

SND-NR (wM-Bus)

Byte No	Field Name	Content	Gas meter example: Bytes [hex] plain	Gas meter example: Bytes [hex] AES coded	Layer
1	L Field	Length of data (67 bytes)		43h	Data Link Layer (DLL)
2	C Field	Send - No Reply		44h	
3	M Field	Manufacturer code		93h	
4	M Field	Manufacturer code		15h	
5	A Field	Ident No LSB (BCD)		78h	
6	A Field	Ident No (BCD)		56h	
7	A Field	Ident No (BCD) (= 12345678)		34h	
8	A Field	Ident No MSB (BCD)		12h	
9	A Field	Version (or Generation number)		33h	
10	A Field	Device type (Gas)		03h	
11	CRC 1			7Ah	
12	CRC 1			C9h	
13	CI Field	Extended Link Layer (short)		8Ch	ELL
14	CC Field	Communication Control		20h	
15	Access No.	ELL-Access Counter of Meter		75h	
16	CI Field	Authentication and Fragmentation layer		90h	Authentication and Fragmentation Layer (AFL)
17	AFLL	AFL Length (all AFL bytes after AFLL)		0Fh	
18	FCL	Fragmentation Control Field (LSB)		00h	
19	FCL	Fragmentation Control Field (MSB)		2Ch	
20	MCL	Message Control Field		25h	
21	MCR	Message Counter C (LSB)		B3h	
22	MCR	Message Counter C		0Ah	
23	MCR	Message Counter C (e.g. = 2739)		00h	
24	MCR	Message Counter C (MSB)		00h	
25	MAC	AES-CMAC (MSB)		21h	
26	MAC	AES-CMAC		92h	
27	MAC	AES-CMAC		4Dh	
28	MAC	AES-CMAC		4Fh	
29	CRC 2			BAh	DLL
30	CRC 2			37h	
31	MAC	AES-CMAC		2Fh	AFL
32	MAC	AES-CMAC		B6h	
33	MAC	AES-CMAC		6Eh	
34	MAC	AES-CMAC (LSB)		01h	
35	CI Field	7Ah (short header)		7Ah	Transport Layer (TPL)
36	Access No.	TPL Access Counter of Meter		75h	
37	Status	Meter status		00h	
38	Config Field	NNNNPIIIb		20h	
39	Config Field	CCZMMMMMb		07h	
40	CFE	0VDDKKKKb		10h	
41	AES-Verify	Decryption verification	2Fh	90h	
42	AES-Verify	Decryption verification	2Fh	58h	
43	DR1	DIF (8 digit BCD)	0Ch	47h	# 1 APL
44	DR1	VIF (Volume 0,01 m³)	14h	5Fh	
45	DR1	Value LSB	27h	4Bh	

46	DR1	Value	04h	C9h		
47	CRC 3			D1h	DLL	
48	CRC 3			28h		
49	DR1	Value (= 28504,27 m³)	85h	1Dh	# 1	Application Layer (APL)
50	DR1	Value MSB	02h	F8h		
51	DR2	DIF (Time at readout; Type F)	04h	78h		
52	DR2	VIF (Date, Time)	6Dh	B8h		
53	DR2	Value LSB	32h	0Ah		
54	DR2	Value	37h	1Bh		
55	DR2	Value (31.05.2008 23:50)	1Fh	0Fh		
56	DR2	Value MSB	15h	98h		
57	DR3	DIF (2 byte integer)	02h	B6h		
58	DR3	VIF (VIF-Extension Table FD)	FDh	29h		
59	DR3	VIFE (error flag)	17h	02h	# 2	
60	DR3	Value LSB	00h	4Ah		
61	DR3	Value MSB (= 0)	00h	ACh		
62	Dummy	Fill Byte due to AES	2Fh	72h		
63	Dummy	Fill Byte due to AES	2Fh	79h		
64	Dummy	Fill Byte due to AES	2Fh	42h		
65	CRC 4			93h	DLL	
66	CRC 4			98h		
67	Dummy	Fill Byte due to AES	2Fh	BFh	# 2	APL
68	Dummy	Fill Byte due to AES	2Fh	C5h		
69	Dummy	Fill Byte due to AES	2Fh	49h		
70	Dummy	Fill Byte due to AES	2Fh	23h		
71	Dummy	Fill Byte due to AES	2Fh	3Ch		
72	Dummy	Fill Byte due to AES	2Fh	01h		
73	Dummy	Fill Byte due to AES	2Fh	40h		
74	Dummy	Fill Byte due to AES	2Fh	82h		
75	Dummy	Fill Byte due to AES	2Fh	9Bh		
76	Dummy	Fill Byte due to AES	2Fh	93h		
77	CRC 5			BAh	DLL	
78	CRC 5			A1h		

N.2.4. wM-Bus Meter with radio adapter and Security profile B

This example shows the communication of a Gas Meter with a bidirectional radio adapter (long TPL) which communicates with a foreign gateway applying long ELL.

Gas meter example	
Medium	Gas
Manufacturer	ELS (1593h)
Ident number	12345678
Version	51
Forward absolute meter volume, temperature converted	28504,27 m³
Date and time of read out	31.05.2008 23:50
Error code binary	0

RF adapter example	
Medium/device type	Radio converter
Manufacturer	RAD (4824h)
Ident number RF-Adapter	11223344
Version	3

Gateway example	
Medium/device type	Comm. controller
Manufacturer	XYZ (633A)
Ident number	33445566
Version	10 (e.g. V 1.0)

5

The Message Counter, the individual Master Key Mk and both derived keys Kenc and Kmac are identical to example N.2.3 wM-Bus Meter with integrated radio and Security profile B.

REQ-UD2 (wM-Bus)

Byte No	Field Name	OMS wM-Bus frame Content	GW -> Gas Bytes [hex] plain	Layer
1	L Field	Length of data (33 bytes)	21h	Data Link Layer (DLL)
2	C Field	Request user data class 2	7Bh	
3	M Field	Manufacturer code	3Ah	
4	M Field	Manufacturer code	63h	
5	A Field	Ident No LSB (BCD)	66h	
6	A Field	Ident No (BCD)	55h	
7	A Field	Ident No (BCD) (=33445566)	44h	
8	A Field	Ident No MSB (BCD) of GW	33h	
9	A Field	Version (or Generation number)	0Ah	
10	A Field	Device type (Medium=COM)	31h	
11	CRC 1		5Dh	
12	CRC 1		17h	
13	CI Field	Extended Link Layer (long)	8Eh	ELL
14	CC Field	Communication Control	84h	
15	Access No.	ELL-Access number of GW	75h	
16	M Field	Manufacturer code	24h	
17	M Field	Manufacturer code	48h	
18	A Field	Ident No LSB (BCD)	44h	
19	A Field	Ident No (BCD)	33h	
20	A Field	Ident No (BCD) (= 11223344)	22h	
21	A Field	Ident No MSB (BCD)	11h	
22	A Field	Version (or Generation number)	03h	
23	A Field	Device type (Communication controller)	37h	
24	CI Field	GW -> Meter	80h	TPL
25	Ident.Nr.	Meter-ID	78h	
26	Ident.Nr.	Meter-ID	56h	
27	Ident.Nr.	Meter-ID	34h	
28	Ident.Nr.	Meter-ID	12h	
29	CRC 2		80h	DLL
30	CRC 2		A4h	
31	Manufr	Meter-Manufacturer-ID	93h	TPL
32	Manufr	Meter-Manufacturer-ID	15h	
33	Version	Meter-Version	33h	
34	Device type	Meter-Device-Type	03h	
35	Access No.	TPL-Access number of GW	75h	
36	Status	GW State RSSI level (-84dBm)	17h	
37	Config Field	0000CCRHb	00h	
38	Config Field	BASMMMMMb	00h	
39	CRC 3		CDh	DLL
40	CRC 3		CDh	

RSP-UD (wM-Bus)

Byte No	Field Name	OMS wM-Bus frame Content	Gas -> GW Bytes [hex] plain	Gas -> GW Bytes [hex] AES coded	Layer
1	L Field	Length of data (83 bytes)		53h	Data Link Layer (DLL)
2	C Field	Respond user data		08h	
3	M Field	Manufacturer code		24h	
4	M Field	Manufacturer code		48h	
5	A Field	Ident No LSB (BCD)		44h	
6	A Field	Ident No (BCD)		33h	
7	A Field	Ident No (BCD) (= 11223344)		22h	
8	A Field	Ident No MSB (BCD)		11h	
9	A Field	Version (or Generation number)		03h	
10	A Field	Device type (Radio converter)		37h	
11	CRC 1			D0h	
12	CRC 1			46h	
13	CI Field	Extended Link Layer (long)		8Eh	ELL
14	CC Field	Communication Control		80h	
15	Access No.	ELL-Access number of GW		75h	
16	M Field	Manufacturer code		3Ah	
17	M Field	Manufacturer code		63h	
18	A Field	Ident No LSB (BCD)		66h	
19	A Field	Ident No (BCD)		55h	
20	A Field	Ident No (BCD) (= 33445566)		44h	
21	A Field	Ident No MSB (BCD)		33h	
22	A Field	Version (or Generation number)		0Ah	
23	A Field	Device type (Communication controller)		31h	
24	CI Field	Authentication and Fragmentation layer		90h	AFL
25	AFLL	AFL Length (all AFL bytes after AFLL)		0Fh	
26	FCL	Fragmentation Control Field (LSB)		00h	
27	FCL	Fragmentation Control Field (MSB)		2Ch	
28	MCL	Message Control Field		25h	
29	CRC 2			E0h	DLL
30	CRC 2			0Ah	
31	MCR	Message Counter C (LSB)		B3h	Authentication and Fragmentation Layer (AFL)
32	MCR	Message Counter C		0Ah	
33	MCR	Message Counter C (e.g. = 2739)		00h	
34	MCR	Message Counter C (MSB)		00h	
35	MAC	AES-CMAC (MSB)		AFh	
36	MAC	AES-CMAC		5Dh	
37	MAC	AES-CMAC		74h	
38	MAC	AES-CMAC		DFh	
39	MAC	AES-CMAC		73h	
40	MAC	AES-CMAC		A6h	
41	MAC	AES-CMAC		00h	
42	MAC	AES-CMAC (LSB)		D9h	
43	CI Field	72h (long header)		72h	TPL
44	Ident.Nr.	Ident No LSB (BCD)		78h	
45	Ident.Nr.	Ident No (BCD)		56h	

46	Ident.Nr.	Ident No (BCD)		34h	
47	CRC 3			C0h	DLL
48	CRC 3			27h	
49	Ident.Nr.	Ident No MSB (BCD) of meter		12h	Transport Layer (TPL)
50	Manufr	Manufacturer code		93h	
51	Manufr	Manufacturer code		15h	
52	Version	Version (or Generation number)		33h	
53	Device type	Device type (Medium = Gas)		03h	
54	Access No.	TPL-Access number of GW		75h	
55	Status	M-Bus state contents errors and alerts		00h	
56	Config Field	NNNNPIIIb		20h	
57	Config Field	CCZMMMMMb		07h	
58	CFE	0VDDKKKKb		10h	
59	AES-Verify	Decryption verification	2Fh	90h	
60	AES-Verify	Decryption verification	2Fh	58h	
61	DR1	DIF (8 digit BCD)	0Ch	47h	# 1 APL
62	DR1	VIF (Volume 0,01 m³)	14h	5Fh	
63	DR1	Value LSB	27h	4Bh	
64	DR1	Value	04h	C9h	
65	CRC 4			55h	DLL
66	CRC 4			CFh	
67	DR1	Value (= 28504,27 m³)	85h	1Dh	# 1 Application Layer (APL)
68	DR1	Value MSB	02h	F8h	
69	DR2	DIF (Time at readout; Type F)	04h	78h	
70	DR2	VIF (Date, Time)	6Dh	B8h	
71	DR2	Value LSB	32h	0Ah	
72	DR2	Value	37h	1Bh	
73	DR2	Value (31.05.2008 23:50)	1Fh	0Fh	
74	DR2	Value MSB	15h	98h	
75	DR3	DIF (2 byte integer)	02h	B6h	
76	DR3	VIF (VIF-Extension Table FD)	FDh	29h	
77	DR3	VIFE (error flag)	17h	02h	# 2
78	DR3	Value LSB	00h	4Ah	
79	DR3	Value MSB (= 0)	00h	ACh	
80	Dummy	Fill Byte due to AES	2Fh	72h	
81	Dummy	Fill Byte due to AES	2Fh	79h	
82	Dummy	Fill Byte due to AES	2Fh	42h	
83	CRC 5			93h	DLL
84	CRC 5			98h	
85	Dummy	Fill Byte due to AES	2Fh	BFh	# 2 APL
86	Dummy	Fill Byte due to AES	2Fh	C5h	
87	Dummy	Fill Byte due to AES	2Fh	49h	
88	Dummy	Fill Byte due to AES	2Fh	23h	
89	Dummy	Fill Byte due to AES	2Fh	3Ch	
90	Dummy	Fill Byte due to AES	2Fh	01h	
91	Dummy	Fill Byte due to AES	2Fh	40h	
92	Dummy	Fill Byte due to AES	2Fh	82h	
93	Dummy	Fill Byte due to AES	2Fh	9Bh	
94	Dummy	Fill Byte due to AES	2Fh	93h	
95	CRC 6			BAh	DLL
96	CRC 6			A1h	

N.2.5. M-Bus Meter with Security profile B

This example shows the communication of a wired M-Bus Gas Meter with Security profile B.

Gas meter example	
Primary address	3
Medium	Gas
Manufacturer	ELS
Ident number	12345678
Version	51
Forward absolute meter volume, temperature converted	28504,27 m³
Date and time of read out	31.05.2008 23:50

5

ToDo:
1. Calculate Session Keys
2. Encrypt Message using Kenc
3. Calculate MAC using Kmac
4. Calculate CS

Individual Master Key Mk (see 9.1):
=00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

Current Message Counter C (LSB first):
= B3 0A 00 00

Encryption Session Key Kenc
= CMAC(Mk, 0x00 || MCR || IdentNo || padding) = CMAC(Mk,00||B3||0A||00||00||78||56||34||12 … ... ||07||07||07||07||07||07||07) = EC CF 39 D4 75 D7 30 B8 28 4F DF DC 19 95 D5 2F

MAC Session Key Kmac
= CMAC(Mk, 0x01 || MCR || IdentNo || padding) = CMAC(Mk,01||B3||0A||00||00||78||56||34||12 … ... ||07||07||07||07||07||07||07) = C9 CD 19 FF 5A 9A AD 5A 6B BD A1 3B D2 C4 C7 AD

RSP-UD (M-Bus)

Byte No	Field Name	OMS M-Bus frame Content	Gas meter example Bytes [hex] plain	Gas meter example Bytes [hex] AES coded	Layer
1	Start	Start byte		68h	Data Link Layer (DLL)
2	L Field	Length of data (49 bytes)		31h	
3	L Field	Length of data (49 bytes)		31h	
4	Start	Start byte		68h	
5	C Field	Respond user data		08h	
6	A Field	Addressing by secondary adress		03h	
7	CI Field	Authentication and Fragmentation layer		90h	Authentication and Fragmentation Layer (AFL)
8	AFLL	AFL Length (all AFL bytes after AFLL)		0Fh	
9	FCL	Fragmentation Control Field (LSB)		00h	
10	FCL	Fragmentation Control Field (MSB)		2Ch	
11	MCL	Message Control Field		25h	
12	MCR	Message Counter C (LSB)		B3h	
13	MCR	Message Counter C		0Ah	
14	MCR	Message Counter C (e.g. = 2739)		00h	
15	MCR	Message Counter C (MSB)		00h	
16	MAC	AES-CMAC (MSB)		A0h	
17	MAC	AES-CMAC		85h	
18	MAC	AES-CMAC		18h	
19	MAC	AES-CMAC		CCh	
20	MAC	AES-CMAC		B0h	
21	MAC	AES-CMAC		22h	
22	MAC	AES-CMAC		C5h	
23	MAC	AES-CMAC (LSB)		FDh	
24	CI Field	72h (long header)		72h	Transport Layer (TPL)
25	Ident.Nr.	Ident No LSB (BCD)		78h	
26	Ident.Nr.	Ident No (BCD)		56h	
27	Ident.Nr.	Ident No (BCD)		34h	
28	Ident.Nr.	Ident No MSB (BCD) of meter		12h	
29	Manufr	Manufacturer code		93h	
30	Manufr	Manufacturer code		15h	
31	Version	Version (or Generation number)		33h	
32	Device type	Device type (Medium = Water)		03h	
33	Access No.	TPL Access Counter of Meter		75h	
34	Status	Meter status		00h	
35	Config Field	NNNNPIIIb		10h	
36	Config Field	CCZMMMMMb		07h	
37	CFE	0VDDKKKKb		10h	
38	AES-Verify	Decryption verification	2Fh	D3h	
39	AES-Verify	Decryption verification	2Fh	71h	
40	DR1	DIF (8 digit BCD)	0Ch	C8h	# 1 APL
41	DR1	VIF (Volume 0,01 m³)	14h	01h	
42	DR1	Value LSB	27h	D4h	
43	DR1	Value	04h	09h	
44	DR1	Value (= 28504,27 m³)	85h	B0h	
45	DR1	Value MSB	02h	D9h	

46	DR2	DIF (Time at readout; Type F)	04h	28h	#1
47	DR2	VIF (Date, Time)	6Dh	D5h	
48	DR2	Value LSB	32h	65h	
49	DR2	Value	37h	97h	
50	DR2	Value (31.05.2008 23:50)	1Fh	59h	
51	DR2	Value MSB	15h	C2h	
52	Dummy	Fill Byte due to AES	2Fh	ECh	
53	Dummy	Fill Byte due to AES	2Fh	93h	
54	Checksum			5Bh	DLL
55	Stop	Stop byte		16h	

N.3 wM-Bus Water Meter with a fragmented message

This example shows a bidirectional water meter, which responds a Compact Load Profile within three fragments to a special request of the GW (e.g. Application select). Data are secured by Security profile B.

N.3.1 Input parameters

Water meter example	
Medium	water
Manufacturer	ZRI
Ident number	12345678
Version	1
Current volume counter	411,979 m3
Current date	18-Aug-2013
Volume counter at due date	383,294 m3
Counter January 2012	345,290 m3
Counter February 2012	347,950 m3
Counter March 2012	351,889 m3
Counter April 2012	355,023 m3
Counter May 2012	358,491 m3
Counter June 2012	362,701 m3
Counter July 2012	365,879 m3
Counter August 2012	371,289 m3
Counter September 2012	373,119 m3
Counter October 2012	375,105 m3
Counter November 2012	377,569 m3
Counter December 2012	381,672 m3

SM-GW example	
Medium/device type	Communication Controller
Manufacturer	XYZ (633A)
Ident number	33445566
Version	10 (e.g. V 1.0)

Individual Master Key Mk (see 9.1):
=00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

Current Message Counter C (LSB first):
= B3 0A 00 00

Encryption Session Key Kenc
= CMAC(Mk, 0x00 || MCR || IdentNo || padding) = CMAC(Mk,00||B3||0A||00||00||78||56||34||12 … … ||07||07||07||07||07||07||07) = EC CF 39 D4 75 D7 30 B8 28 4F DF DC 19 95 D5 2F

MAC Session Key Kmac
= CMAC(Mk, 0x01 || MCR || IdentNo || padding) = CMAC(Mk,01||B3||0A||00||00||78||56||34||12 … ... ||07||07||07||07||07||07||07) = C9 CD 19 FF 5A 9A AD 5A 6B BD A1 3B D2 C4 C7 AD

Notes
The selected fragment sizes have been chosen disproportionately short to obtain the clarity of example. To avoid unefficient channel use a larger fragments size should be selected.

N.3.2 Calculate Message

To build a message following order has to be applied.

1. Derive Kenc and Kmac
2. Encrypt the message with Kenc
3. Calculate a 16 Byte CMAC with Kmac
   (Note for a truncated CMAC the first 8 bytes are used only)
4. Separate message in several fragments
5. Add lower layers (AFL, ELL, DLL)
6. Calculate length and CRC

Encryption and Authentication over the Message

	unfragmented message	Water meter example				
Field Name	Content	Bytes [hex]	Bytes [hex]			
		plain	AES coded			
MCL	MLMP=1, MCMP=1, AES128-CMAC, 8 bytes	65h	65h		Fields to be considered by the CMAC-Calculation	Fragment 1 (length = 26 bytes)
MCR	Message Counter (LSB)	B3h	B3h			
MCR	Message Counter (eg. 2739)	0Ah	0Ah			
MCR	Message Counter	00h	00h			
MCR	Message Counter (MSB)	00h	00h			
ML	Message Length (LSB) = 86 bytes	56h	56h			
ML	Message Length (MSB)	00h	00h			
CI Field	Short header	7Ah	7Ah			
ACC	Access Counter	05h	05h			
Status	Status byte	00h	00h			
Config Field	NNNNPIIIb (5 blocks)	50h	50h			
Config Field	CCZMMMMMb (Enc. mode 7, no signature in APL)	07h	07h			
CFE	0VDDKKKKb (dyn. Key)	10h	10h			
Decr. Verify	Decryption verfication	2Fh	30h			
Decr. Verify	Decryption verfication	2Fh	53h			
DR1	DIF storage #0, 8 digit BCD	0Ch	9Ah	# 1		
DR1	VIF volume liter	13h	7Ch			
DR1	Value current volume (LSB)	79h	DBh			
DR1	Value current volume	19h	1Ch			
DR1	Value current volume	41h	BCh			
DR1	Value current volume (MSB)	00h	A6h			
DR2	DIF storage #0, 16bit	02h	D4h			
DR2	VIF date type G, acc. to EN13757-3, Annex A	6Ch	3Ch	# 1	th	ng

DR2	Value current date (LSB)	B2h	B0h			
DR2	Value current date (MSB)	18h	2Dh			
DR3	DIF Storage #1, 8 digit BCD	4Ch	76h			
DR3	VIF volume liter	13h	2Ah			
DR3	Value due date volume (LSB)	94h	1Eh			
DR3	Value due date volume	32h	16h			
DR3	Value due date volume	38h	26h	# 2		
DR3	Value due date volume (MSB)	00h	FEh			
DR4	DIF base time, 16 bit	82h	EFh			
DR4	DIFE storage #8, as required by EN13757-3, Annex I	04h	0Eh			
DR4	VIF date type G, acc. to EN13757-3, Annex A	6Ch	C4h			Fragment 2 (length = 33 bytes)
DR4	Value base date (LSB) 1-Jan-2012	81h	90h			
DR4	Value base date (MSB)	11h	27h			
DR5	DIF base value, 8 digit BCD	8Ch	8Eh			
DR5	DIFE storage #8	04h	41h			
DR5	VIF volume liter	13h	A4h			
DR5	Value (LSB)	90h	8Bh			
DR5	Value	52h	ADh			
DR5	Value	34h	14h			
DR5	Value (MSB)	00h	38h			
DR6	DIF variable length	8Dh	BDh			
DR6	DIFE storage #8	04h	E3h			
DR6	VIF volume liter	93h	8Dh	# 3		
DR6	orthogonal VIFE, compact profile without registers	1Fh	4Dh			
DR6	LVAR length of profile (2+11*3 = 35 Bytes)	23h	11h			
DR6	Spacing control: signed difference, month, 6 digit BCD	FBh	66h			
DR6	Spacing value: month, acc. to Annex I table I.9	FEh	30h			
DR6	Value (LSB)	60h	5Dh			
DR6	Value n-11 (February)	26h	EFh			
DR6	Value (MSB)	00h	F6h			
DR6	Value (LSB)	39h	39h			
DR6	Value n-10 (March)	39h	2Bh			
DR6	Value (MSB)	00h	6Bh			
DR6	Value (LSB)	34h	E3h			
DR6	Value n-9 (April)	31h	1Ah			
DR6	Value (MSB)	00h	9Fh			
DR6	Value (LSB)	68h	C8h			
DR6	Value n-8 (May)	34h	12h			
DR6	Value (MSB)	00h	75h	# 4		
DR6	Value (LSB)	10h	7Bh			
DR6	Value n-7 (June)	42h	E8h			
DR6	Value (MSB)	00h	05h			
DR6	Value (LSB)	78h	B4h			

DR6	Value n-6 (July)	31h	06h	# 4	Fields to be considered by the CMAC-Calculation	Fragment 3 (length = 27 bytes)
DR6	Value (MSB)	00h	CCh			
DR6	Value (LSB)	10h	3Eh			
DR6	Value n-5 (August)	54h	04h			
DR6	Value (MSB)	00h	57h			
DR6	Value (LSB)	30h	C7h			
DR6	Value n-4 (September)	18h	25h			
DR6	Value (MSB)	00h	B4h			
DR6	Value (LSB)	86h	B2h			
DR6	Value n-3 (October)	19h	9Bh			
DR6	Value (MSB)	00h	E7h			
DR6	Value (LSB)	64h	FEh	# 5		
DR6	Value n-2 (November)	24h	F0h			
DR6	Value (MSB)	00h	78h			
DR6	Value (LSB)	03h	77h			
DR6	Value n-1 (December)	41h	71h			
DR6	Value (MSB)	00h	87h			
DR7	DIF 16bit	02h	CCh			
DR7	VIF from FD table	FDh	EFh			
DR7	VIFE error flags, device specific	17h	8Eh			
DR7	Value error flags byte A	00h	2Ah			
DR7	Value error flags byte B	00h	F5h			
Dummy	Idle filler	2Fh	1Ch			
Dummy	Idle filler	2Fh	C7h			
Dummy	Idle filler	2Fh	29h			
Dummy	Idle filler	2Fh	EFh			
Dummy	Idle filler	2Fh	7Ah			
MAC	MAC (MSB)		BEh			
MAC	MAC		47h			
MAC	MAC		EDh			
MAC	MAC		4Ch			
MAC	MAC		9Ch			
MAC	MAC		C1h			
MAC	MAC		1Ah			
MAC	MAC		78h			
MAC	MAC		58h			
MAC	MAC		14h			
MAC	MAC		48h			
MAC	MAC		F6h			
MAC	MAC		77h			
MAC	MAC		46h			
MAC	MAC		00h			
MAC	MAC (LSB)		EEh			

N.3.3 First fragment

After the REQ-UD2 the first fragment is responded. The Message length indicates the total length of the unfragmented message. The More Fragment Bit (MF=1) in the AFL informs the GW that more fragments has to be requested.

5

REQ-UD2 (wM-Bus - Fragment 1)

		OMS wM-Bus frame	GW -> MTR	Layer
Byte No	Field Name	Content	Bytes [hex]	
			plain	
1	L Field	Length of data (25 bytes)	19h	Data Link Layer (DLL)
2	C Field	Request user data class 2	7Bh	
3	M Field	Manufacturer code	3Ah	
4	M Field	Manufacturer code	63h	
5	A Field	Ident No LSB (BCD)	66h	
6	A Field	Ident No (BCD)	55h	
7	A Field	Ident No (BCD) (=33445566)	44h	
8	A Field	Ident No MSB (BCD) of GW	33h	
9	A Field	Version (or Generation number)	0Ah	
10	A Field	Device type (Medium=COM)	31h	
11	CRC 1		82h	
12	CRC 1		2Eh	
13	CI Field	Extended Link Layer (short)	8Ch	ELL
14	CC Field	Communication Control	84h	
15	Access No.	Access Number of GW	11h	
16	CI Field	GW -> Meter	80h	Transport Layer (TPL)
17	Ident.Nr.	Meter-ID	78h	
18	Ident.Nr.	Meter-ID	56h	
19	Ident.Nr.	Meter-ID	34h	
20	Ident.Nr.	Meter-ID	12h	
21	Manufr	Meter-Manufacturer-ID	49h	
22	Manufr	Meter-Manufacturer-ID	6Ah	
23	Version	Meter-Version	01h	
24	Device type	Meter-Device-Type	07h	
25	Access No.	Access Number of GW	05h	
26	Status	GW State RSSI level (-84dBm)	17h	
27	Config Field	0000CCRHb	00h	
28	Config Field	BASMMMMMb (no encr.)	00h	
29	CRC 2		CBh	DLL
30	CRC 2		20h	

RSP-UD (wM-Bus - Fragment1)

Byte No	Field Name	Content	MTR->GW Bytes [hex] plain	MTR->GW Bytes [hex] AES coded	Layer
1	L Field	Length of data (57 bytes)		39h	DLL
2	C Field	Respond user data		08h	
3	M Field	Manufacturer code ZRI (LSB)		49h	
4	M Field	Manufacturer code (MSB)		6Ah	
5	A Field	Ident No LSB (BCD)		78h	
6	A Field	Ident No (BCD)		56h	
7	A Field	Ident No (BCD) (= 12345678)		34h	
8	A Field	Ident No MSB (BCD)		12h	
9	A Field	Version (or Generation number)		01h	
10	A Field	Device type water meter		07h	
11	CRC 1			14h	
12	CRC 1			64h	
13	CI Field	Extended LinkLayer		8Eh	ELL
14	CC Field	Communication Control (bidir.)		80h	
15	Access No.	ELL-Access number of Meter		11h	
16	M Field	Manufacturer code		3Ah	
17	M Field	Manufacturer code		63h	
18	A Field	Ident No LSB (BCD)		66h	
19	A Field	Ident No (BCD)		55h	
20	A Field	Ident No (BCD) (= 33445566)		44h	
21	A Field	Ident No MSB (BCD)		33h	
22	A Field	Version (or Generation number)		0Ah	
23	A Field	Device type (Communication controller)		31h	
24	CI Field	Authentification & Fragmentation Layer (AFL)		90h	AFL
25	AFLL	AFL Length Field		09h	
26	FCL	FID, Fragment-ID		01h	
27	FCL	MF=1, MCLP=1, MLP=1, MCRP=1, MACP=0		78h	
28	MCL	MLMP=1, MCMP=1, AES128-CMAC, 8 bytes		65h	
29	CRC 2			D4h	DLL
30	CRC 2			38h	
31	MCR	Message Counter C (LSB)		B3h	AFL
32	MCR	Message Counter C (eg. 2739)		0Ah	
33	MCR	Message Counter C		00h	
34	MCR	Message Counter C (MSB)		00h	
35	ML	Message Length (LSB) = 86 bytes		56h	
36	ML	Message Length (MSB)		00h	
37	CI Field	Short header		7Ah	TPL
38	Access No.	TPL Access number of Meter		05h	
39	Status	Status byte		00h	
40	Config Field	NNNNPIIIb		50h	
41	Config Field	CCZMMMMMb (encr. mode 7, no signature in APL)		07h	
42	CFE	0VDDKKKKb (dyn. Key)		10h	
43	Decr. Verify	Decryption verfication	2Fh	30h	
44	Decr. Verify	Decryption verfication	2Fh	53h	

45	DR1	DIF storage #0, 8 digit BCD	0Ch	9Ah	# 1	APL
46	DR1	VIF volume liter	13h	7Ch		
47	CRC 3			63h	DLL	
48	CRC 3			ABh		
49	DR1	Value current volume (LSB)	79h	DBh	# 1	APL
50	DR1	Value current volume	19h	1Ch		
51	DR1	Value current volume	41h	BCh		
52	DR1	Value current volume (MSB)	00h	A6h		
53	DR2	DIF storage #0, 16bit	02h	D4h		
54	DR2	VIF date type G, acc. to EN13757-3, Annex A	6Ch	3Ch		
55	DR2	Value current date (LSB)	B2h	B0h		
56	DR2	Value current date (MSB)	18h	2Dh		
57	DR3	DIF Storage #1, 8 digit BCD	4Ch	76h		
58	DR3	VIF volume liter	13h	2Ah		
59	DR3	Value due date volume (LSB)	94h	1Eh		
60	DR3	Value due date volume	32h	16h		
61	DR3	Value due date volume	38h	26h	# 2	
62	DR3	Value due date volume (MSB)	00h	FEh		
63	DR4	DIF base time, 16 bit	82h	EFh		
64	DR4	DIFE storage #8, acc. to EN13757-3, Annex I	04h	0Eh		
65	CRC 4			8Eh	DLL	
66	CRC 4			95h		

N.3.4 Second fragment

REQ-UD2 (wM-Bus - Fragment 2)

Byte No	Field Name	OMS wM-Bus frame Content	GW -> MTR Bytes [hex] plain	Layer
1	L Field	Length of data (20 bytes)	14h	Data Link Layer (DLL)
2	C Field	Request user data class 2	5Bh	
3	M Field	Manufacturer code	3Ah	
4	M Field	Manufacturer code	63h	
5	A Field	Ident No LSB (BCD)	66h	
6	A Field	Ident No (BCD)	55h	
7	A Field	Ident No (BCD) (=33445566)	44h	
8	A Field	Ident No MSB (BCD) of GW	33h	
9	A Field	Version (or Generation number)	0Ah	
10	A Field	Device type (Medium=COM)	31h	
11	CRC 1		47h	
12	CRC 1		39h	
13	CI Field	Extended Link Layer (long)	8Eh	ELL
14	CC Field	Communication Control	84h	
15	Access No.	ELL-Access number of GW	12h	
16	M Field	Manufacturer code	49h	
17	M Field	Manufacturer code	6Ah	
18	A Field	Ident No LSB (BCD)	78h	
19	A Field	Ident No (BCD)	56h	
20	A Field	Ident No (BCD) (= 12345678)	34h	
21	A Field	Ident No MSB (BCD)	12h	
22	A Field	Version	01h	
23	A Field	Device type water meter	07h	
24	CRC 2		53h	DLL
25	CRC 2		CFh	

RSP-UD (wM-Bus - Fragment2)

Byte No	Field Name	OMS wM-Bus frame (intermediate fragment)	MTR->GW Bytes [hex] plain	Bytes [hex] AES coded	Layer
1	L Field	Length of data (57 bytes)		39h	DLL
2	C Field	Respond user data		08h	
3	M Field	Manufacturer code ZRI (LSB)		49h	
4	M Field	Manufacturer code (MSB)		6Ah	
5	A Field	Ident No LSB (BCD)		78h	
6	A Field	Ident No (BCD)		56h	
7	A Field	Ident No (BCD) (= 12345678)		34h	
8	A Field	Ident No MSB (BCD)		12h	
9	A Field	Version (or Generation number)		01h	
10	A Field	Device type water meter		07h	
11	CRC 1			14h	
12	CRC 1			64h	
13	CI Field	Extended LinkLayer		8Eh	ELL
14	CC Field	Communication Control (bidir.)		80h	
15	Access No.	ELL-Access number of Meter		12h	
16	M Field	Manufacturer code		3Ah	
17	M Field	Manufacturer code		63h	
18	A Field	Ident No LSB (BCD)		66h	
19	A Field	Ident No (BCD)		55h	
20	A Field	Ident No (BCD) (= 33445566)		44h	
21	A Field	Ident No MSB (BCD)		33h	
22	A Field	Version (or Generation number)		0Ah	
23	A Field	Device type (Communication controller)		31h	
24	CI Field	AFL		90h	AFL
25	AFLL	AFL Length Field		02h	
26	FCL	FID, Fragment-ID		02h	
27	FCL	MF=1, MCLP=0, MLP=0, MCRP=0, MACP=0		40h	
28	DR4	VIF date type G, acc. to EN13757-3, Annex A	6Ch	C4h	APL
29	CRC 2			E9h	DLL
30	CRC 2			B3h	
31	DR4	Value base date (LSB) 1-Jan-2012	81h	90h	APL # 2
32	DR4	Value base date (MSB)	11h	27h	
33	DR5	DIF base value, 8 digit BCD	8Ch	8Eh	
34	DR5	DIFE storage #8	04h	41h	
35	DR5	VIF volume liter	13h	A4h	
36	DR5	Value (LSB)	90h	8Bh	
37	DR5	Value	52h	ADh	
38	DR5	Value	34h	14h	
39	DR5	Value (MSB)	00h	38h	
40	DR6	DIF variable length	8Dh	BDh	
41	DR6	DIFE storage #8	04h	E3h	
42	DR6	VIF volume liter	93h	8Dh	APL # 3
43	DR6	orth. VIFE, compact profile without registers	1Fh	4Dh	
44	DR6	LVAR length of profile (2+11*3 = 35 Bytes)	23h	11h	
45	DR6	Spacing control: signed diff., month, 6 digit BCD	FBh	66h	
46	DR6	Spacing value: month, acc. to Annex I table I.9	FEh	30h	

47	CRC 3			21h	DLL
48	CRC 3			5Fh	
49	DR6	Value (LSB)	60h	5Dh	# 3 / APL
50	DR6	Value n-11 (February)	26h	EFh	
51	DR6	Value (MSB)	00h	F6h	
52	DR6	Value (LSB)	39h	39h	
53	DR6	Value n-10 (March)	39h	2Bh	
54	DR6	Value (MSB)	00h	6Bh	
55	DR6	Value (LSB)	34h	E3h	
56	DR6	Value n-9 (April)	31h	1Ah	
57	DR6	Value (MSB)	00h	9Fh	
58	DR6	Value (LSB)	68h	C8h	
59	DR6	Value n-8 (May)	34h	12h	
60	DR6	Value (MSB)	00h	75h	# 4 / APL
61	DR6	Value (LSB)	10h	7Bh	
62	DR6	Value n-7 (June)	42h	E8h	
63	DR6	Value (MSB)	00h	05h	
64	DR6	Value (LSB)	78h	B4h	
65	CRC 4			B1h	DLL
66	CRC 4			86h	

N.3.5 Last fragment

The clear More Fragment Bit indicates the last Fragment. This datagram contains also the CMAC of the message.

REQ-UD2 (wM-Bus - Fragment 3)

Byte No		OMS wM-Bus frame	GW -> MTR	Layer
	Field Name	Content	Bytes [hex]	
			plain	
1	L Field	Length of data (20 bytes)	14h	Data Link Layer (DLL)
2	C Field	Request user data class 2	7Bh	
3	M Field	Manufacturer code	3Ah	
4	M Field	Manufacturer code	63h	
5	A Field	Ident No LSB (BCD)	66h	
6	A Field	Ident No (BCD)	55h	
7	A Field	Ident No (BCD) (=33445566)	44h	
8	A Field	Ident No MSB (BCD) of GW	33h	
9	A Field	Version (or Generation number)	0Ah	
10	A Field	Device type (Medium=COM)	31h	
11	CRC 1		B6h	
12	CRC 1		0Ch	
13	CI Field	Extended Link Layer (long)	8Eh	ELL
14	CC Field	Communication Control	84h	
15	Access No.	ELL-Access number of GW	13h	
16	M Field	Manufacturer code	49h	
17	M Field	Manufacturer code	6Ah	
18	A Field	Ident No LSB (BCD)	78h	
19	A Field	Ident No (BCD)	56h	
20	A Field	Ident No (BCD) (= 12345678)	34h	
21	A Field	Ident No MSB (BCD)	12h	
22	A Field	Version	01h	
23	A Field	Device type water meter	07h	
24	CRC 2		C3h	DLL
25	CRC 2		1Fh	

5

RSP-UD (wM-Bus - Fragment3)

		OMS wM-Bus frame (last fragment)	MTR->GW		Layer
Byte No	Field Name	Content	Bytes [hex]	Bytes [hex]	
			plain	AES coded	
1	L Field	Length of data (59 bytes)		3Bh	DLL
2	C Field	Respond user data		08h	
3	M Field	Manufacturer code ZRI (LSB)		49h	
4	M Field	Manufacturer code (MSB)		6Ah	
5	A Field	Ident No LSB (BCD)		78h	
6	A Field	Ident No (BCD)		56h	
7	A Field	Ident No (BCD) (= 12345678)		34h	
8	A Field	Ident No MSB (BCD)		12h	
9	A Field	Version (or Generation number)		01h	
10	A Field	Device type water meter		07h	
11	CRC 1			63h	
12	CRC 1			42h	
13	CI Field	Extended LinkLayer		8Eh	ELL
14	CC Field	Communication Control (bidir.)		80h	
15	Access No.	ELL-Access number of Meter		13h	
16	M Field	Manufacturer code		3Ah	
17	M Field	Manufacturer code		63h	
18	A Field	Ident No LSB (BCD)		66h	
19	A Field	Ident No (BCD)		55h	
20	A Field	Ident No (BCD) (= 33445566)		44h	
21	A Field	Ident No MSB (BCD)		33h	
22	A Field	Version (or Generation number)		0Ah	
23	A Field	Device type (Communication controller)		31h	
24	CI Field	AFL		90h	AFL
25	AFLL	AFL Length Field		0Ah	
26	FCL	FID, Fragment-ID		03h	
27	FCL	MF=0, MCLP=0, MLP=0, MCRP=0, MACP=1		04h	
28	MAC	MAC (MSB)		BEh	
29	CRC 2			41h	DLL
30	CRC 2			AFh	
31	MAC	MAC		47h	AFL
32	MAC	MAC		EDh	
33	MAC	MAC		4Ch	
34	MAC	MAC		9Ch	
35	MAC	MAC		C1h	
36	MAC	MAC		1Ah	
37	MAC	MAC (LSB)		78h	
38	DR6	Value n-6 (July)	31h	06h	# 4 APL
39	DR6	Value (MSB)	00h	CCh	
40	DR6	Value (LSB)	10h	3Eh	
41	DR6	Value n-5 (August)	54h	04h	
42	DR6	Value (MSB)	00h	57h	
43	DR6	Value (LSB)	30h	C7h	
44	DR6	Value n-4 (September)	18h	25h	
45	DR6	Value (MSB)	00h	B4h	
46	DR6	Value (LSB)	86h	B2h	

47	CRC 3			CDh	DLL	
48	CRC 3			8Ch		
49	DR6	Value n-3 (October)	19h	9Bh	# 4	APL
50	DR6	Value (MSB)	00h	E7h		
51	DR6	Value (LSB)	64h	FEh	# 5	
52	DR6	Value n-2 (November)	24h	F0h		
53	DR6	Value (MSB)	00h	78h		
54	DR6	Value (LSB)	03h	77h		
55	DR6	Value n-1 (December)	41h	71h		
56	DR6	Value (MSB)	00h	87h		
57	DR7	DIF 16bit	02h	CCh		
58	DR7	VIF from FD table	FDh	EFh		
59	DR7	VIFE error flags, device specific	17h	8Eh		
60	DR7	Value error flags byte A	00h	2Ah		
61	DR7	Value error flags byte B	00h	F5h		
62	Dummy	Idle filler	2Fh	1Ch		
63	Dummy	Idle filler	2Fh	C7h		
64	Dummy	Idle filler	2Fh	29h		
65	CRC 4			95h	DLL	
66	CRC 4			83h		
67	Dummy	Idle filler	2Fh	EFh	# 5	APL
68	Dummy	Idle filler	2Fh	7Ah		
69	CRC 5			C7h	DLL	
70	CRC 5			F2h		

N.4 M-Bus Water Meter with a fragmented message

This example shows a wired M-Bus water meter, which responds a Compact Load Profile within three fragments to a special request of the GW (e.g. Application select). Data are secured by Security profile A.

N.4.1 Input parameters

Water meter example	
Primary address	3
Medium	water
Manufacturer	QDS
Ident number	12345678
Version	16
Current volume counter	411,979 m3
Current date	18-Aug-2013
Volume counter at due date	383,294 m3
Counter January 2012	345,290 m3
Counter February 2012	347,950 m3
Counter March 2012	351,889 m3
Counter April 2012	355,023 m3
Counter May 2012	358,491 m3
Counter June 2012	362,701 m3
Counter July 2012	365,879 m3
Counter August 2012	371,289 m3
Counter September 2012	373,119 m3
Counter October 2012	375,105 m3
Counter November 2012	377,569 m3
Counter December 2012	381,672 m3

SM-GW example	
Medium/device type	Communication Controller
Manufacturer	XYZ (633A)
Ident number	33445566
Version	10 (e.g. V 1.0)

AES Key according to FIPS 197 (see 9.1):
=00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

AES CBC Initial Vector according to FIPS 197 (LSB first):
= M Field + A Field + 8 bytes Acces No = 93 44 78 56 34 12 10 07 05 05 05 05 05 05 05 05

Notes
The selected fragment sizes have been chosen disproportionately short to obtain the clarity of example. To avoid unefficient channel use a larger fragments size should be selected.

N.4.2 Calculate Message

To build a message following order has to be applied.

1. Separate message in several fragments
2. Add lower layers (AFL, DLL)
3. Calculate length and CRC

Encryption over the Message

	unfragmented message	Water meter example				
Field Name	Content	Bytes [hex] plain	Bytes [hex] AES coded			
MCL	MLMP=1, MCMP=0, AT=00; ATO=00	40h	40h		Total Message	Fragment 1 (length = 36 bytes)
ML	Message Length (LSB) = 93 bytes	5Dh	5Dh			
ML	Message Length (MSB)	00h	00h			
CI Field	72h (long header)	72h	72h			
Ident.Nr.	Ident No LSB (BCD)	78h	78h			
Ident.Nr.	Ident No (BCD)	56h	56h			
Ident.Nr.	Ident No (BCD)	34h	34h			
Ident.Nr.	Ident No MSB (BCD) of meter	12h	12h			
Manufr	Manufacturer code	93h	93h			
Manufr	Manufacturer code	44h	44h			
Version	Version (or Generation number)	10h	10h			
Device type	Device type (Medium = Water)	07h	07h			
ACC	Access Counter	05h	05h			
Status	Status byte	00h	00h			
Config Field	NNNNCCRHb (5 blocks)	00h	50h			
Config Field	BASMMMMMb (Enc. mode 5, no signature in APL)	00h	05h			
Decr. Verify	Decryption verfication	2Fh	28h			
Decr. Verify	Decryption verfication	2Fh	FCh			
DR1	DIF storage #0, 8 digit BCD	0Ch	B7h	# 1		
DR1	VIF volume liter	13h	63h			
DR1	Value current volume (LSB)	79h	E5h			
DR1	Value current volume	19h	1Bh			
DR1	Value current volume	41h	4Ah			
DR1	Value current volume (MSB)	00h	6Dh			
DR2	DIF storage #0, 16bit	02h	4Fh			
DR2	VIF date type G, acc. to EN13757-3, Annex A	6Ch	DDh			
DR2	Value current date (LSB)	B2h	F2h			
DR2	Value current date (MSB)	18h	EEh			
DR3	DIF Storage #1, 8 digit BCD	4Ch	A9h			
DR3	VIF volume liter	13h	06h	#1		

DR3	Value due date volume (LSB)	94h	F6h			
DR3	Value due date volume	32h	1Eh			
DR3	Value due date volume	38h	D0h	#2		
DR3	Value due date volume (MSB)	00h	DAh			
DR4	DIF base time, 16 bit	82h	7Ah			
DR4	DIFE storage #8, as required by EN13757-3, Annex I	04h	B2h			
DR4	VIF date type G, acc. to EN13757-3, Annex A	6Ch	97h			Fragment 2 (length = 33 bytes)
DR4	Value base date (LSB) 1-Jan-2012	81h	87h			
DR4	Value base date (MSB)	11h	E1h			
DR5	DIF base value, 8 digit BCD	8Ch	B2h			
DR5	DIFE storage #8	04h	B5h			
DR5	VIF volume liter	13h	E3h			
DR5	Value (LSB)	90h	4Eh			
DR5	Value	52h	F3h			
DR5	Value	34h	C5h			
DR5	Value (MSB)	00h	90h			
DR6	DIF variable length	8Dh	3Eh			
DR6	DIFE storage #8	04h	3Ah			
DR6	VIF volume liter	93h	E4h	#3		
DR6	orthogonal VIFE, compact profile without registers	1Fh	24h			
DR6	LVAR length of profile (2+11*3 = 35 Bytes)	23h	27h			
DR6	Spacing control: signed difference, month, 6 digit BCD	FBh	CDh			
DR6	Spacing value: month, acc. to Annex I table I.9	FEh	A9h			
DR6	Value (LSB)	60h	DBh			
DR6	Value n-11 (February)	26h	24h			
DR6	Value (MSB)	00h	07h			
DR6	Value (LSB)	39h	FAh			
DR6	Value n-10 (March)	39h	81h			
DR6	Value (MSB)	00h	31h			
DR6	Value (LSB)	34h	EFh			
DR6	Value n-9 (April)	31h	B2h			
DR6	Value (MSB)	00h	25h			
DR6	Value (LSB)	68h	97h			
DR6	Value n-8 (May)	34h	98h			
DR6	Value (MSB)	00h	E2h	#4		
DR6	Value (LSB)	10h	B7h			
DR6	Value n-7 (June)	42h	9Bh			
DR6	Value (MSB)	00h	AAh			
DR6	Value (LSB)	78h	D1h			
DR6	Value n-6 (July)	31h	AFh			
DR6	Value (MSB)	00h	89h			
DR6	Value (LSB)	10h	B7h			
DR6	Value n-5 (August)	54h	50h			
DR6	Value (MSB)	00h	6Fh			
DR6	Value (LSB)	30h	EBh			
DR6	Value n-4 (September)	18h	16h			
DR6	Value (MSB)	00h	C2h			
DR6	Value (LSB)	86h	2Bh			
DR6	Value n-3 (October)	19h	15h			
DR6	Value (MSB)	00h	1Bh			
DR6	Value (LSB)	64h	35h	#5	M	Fragment 3 (length = 27 bytes)

DR6	Value n-2 (November)	24h	37h			
DR6	Value (MSB)	00h	FAh			
DR6	Value (LSB)	03h	27h			
DR6	Value n-1 (December)	41h	2Dh			
DR6	Value (MSB)	00h	55h			
DR7	DIF 16bit	02h	22h			
DR7	VIF from FD table	FDh	75h			
DR7	VIFE error flags, device specific	17h	62h			
DR7	Value error flags byte A	00h	C6h			
DR7	Value error flags byte B	00h	3Fh			
Dummy	Idle filler	2Fh	6Ch			
Dummy	Idle filler	2Fh	40h			
Dummy	Idle filler	2Fh	83h			
Dummy	Idle filler	2Fh	83h			
Dummy	Idle filler	2Fh	EBh			

N.4.3 First fragment

After the REQ-UD2 the first fragment is responded. The Message length indicates to total length of the unfragmented message. The More Fragment Bit in the AFL informs the GW that more fragments has to be requested.

5

REQ-UD2 (M-Bus - Fragment 1)

Byte No		OMS M-Bus frame	GW -> MTR	Layer
	Field Name	Content	Bytes [hex]	
			plain	
1	Start	Start byte	10h	DLL
2	C Field	Respond user data	7Bh	
3	A Field	Addressing by secondary address	FDh	
4	Checksum		78h	
5	Stop	Stop byte	16h	

RSP-UD (M-Bus - Fragment1)

Byte No		OMS M-Bus frame (first fragment)	MTR->GW		Layer
	Field Name	Content	Bytes [hex]	Bytes [hex]	
			plain	AES coded	
1	Start	Start byte		68h	DLL
2	L Field	Length of data (42 bytes)		2Ah	
3	L Field	Length of data (42 bytes)		2Ah	
4	Start	Start byte		68h	
5	C Field	Respond user data		08h	
6	A Field	Addressing by secondary address		03h	
7	CI Field	Authentification & Fragmentation Layer (AFL)		90h	AFL
8	AFLL	AFL Length Field		05h	
9	FCL	FID, Fragment-ID		01h	
10	FCL	MF=1, MCLP=1, MLP=1, MCRP=0, MACP=0		70h	
11	MCL	MLMP=1, MCMP=0, AT=00; ATO=00		40h	
12	ML	Message Length (LSB) = 93 bytes		5Dh	
13	ML	Message Length (MSB)		00h	
14	CI Field	72h (long header)		72h	TPL
15	Ident.Nr.	Ident No LSB (BCD)		78h	
16	Ident.Nr.	Ident No (BCD)		56h	
17	Ident.Nr.	Ident No (BCD)		34h	
18	Ident.Nr.	Ident No MSB (BCD) of meter		12h	
19	Manufr	Manufacturer code		93h	
20	Manufr	Manufacturer code		44h	
21	Version	Version (or Generation number)		10h	
22	Device type	Device type (Medium = Water)		07h	
23	Access No.	TPL Access number of Meter		05h	
24	Status	Status byte		00h	
25	Config Field	NNNNCCRHb (5 blocks)		50h	
26	Config Field	BASMMMMMb (encr. mode 5, no signature in APL)		05h	
27	Decr. Verify	Decryption verfication	2Fh	28h	
28	Decr. Verify	Decryption verfication	2Fh	FCh	

29	DR1	DIF storage #0, 8 digit BCD	0Ch	B7h	# 1	APL
30	DR1	VIF volume liter	13h	63h		
31	DR1	Value current volume (LSB)	79h	E5h		
32	DR1	Value current volume	19h	1Bh		
33	DR1	Value current volume	41h	4Ah		
34	DR1	Value current volume (MSB)	00h	6Dh		
35	DR2	DIF storage #0, 16bit	02h	4Fh		
36	DR2	VIF date type G, acc. to EN13757-3, Annex A	6Ch	DDh		
37	DR2	Value current date (LSB)	B2h	F2h		
38	DR2	Value current date (MSB)	18h	EEh		
39	DR3	DIF Storage #1, 8 digit BCD	4Ch	A9h		
40	DR3	VIF volume liter	13h	06h		
41	DR3	Value due date volume (LSB)	94h	F6h		
42	DR3	Value due date volume	32h	1Eh		
43	DR3	Value due date volume	38h	D0h	# 2	
44	DR3	Value due date volume (MSB)	00h	DAh		
45	DR4	DIF base time, 16 bit	82h	7Ah		
46	DR4	DIFE storage #8, acc. to EN13757-3, Annex I	04h	B2h		
47	Checksum			16h	DLL	
48	Stop	Stop byte		16h		

N.4.4 Second fragment

REQ-UD2 (wM-Bus - Fragment 2)

Byte No		OMS M-Bus frame	GW -> MTR	Layer
	Field Name	Content	Bytes [hex]	
			plain	
1	Start	Start byte	10h	DLL
2	C Field	Respond user data	5Bh	
3	A Field	Addressing by secondary address	FDh	
4	Checksum		58h	
5	Stop	Stop byte	16h	

RSP-UD (M-Bus - Fragment2)

Byte No		OMS M-Bus frame (intermediate fragment)	MTR->GW		Layer	
	Field Name	Content	Bytes [hex]	Bytes [hex]		
			plain	AES coded		
1	Start	Start byte		68h	DLL	
2	L Field	Length of data (39 bytes)		27h		
3	L Field	Length of data (39 bytes)		27h		
4	Start	Start byte		68h		
5	C Field	Respond user data		08h		
6	A Field	Addressing by secondary adress		03h		
7	CI Field	AFL		90h	AFL	
8	AFLL	AFL Length Field		02h		
9	FCL	FID, Fragment-ID		02h		
10	FCL	MF=1, MCLP=0, MLP=0, MCRP=0, MACP=0		40h		
11	DR4	VIF date type G, acc. to EN13757-3, Annex A	6Ch	97h	# 2	APL
12	DR4	Value base date (LSB) 1-Jan-2012	81h	87h		
13	DR4	Value base date (MSB)	11h	E1h		
14	DR5	DIF base value, 8 digit BCD	8Ch	B2h		
15	DR5	DIFE storage #8	04h	B5h		
16	DR5	VIF volume liter	13h	E3h		
17	DR5	Value (LSB)	90h	4Eh		
18	DR5	Value	52h	F3h		
19	DR5	Value	34h	C5h		
20	DR5	Value (MSB)	00h	90h		
21	DR6	DIF variable length	8Dh	3Eh		
22	DR6	DIFE storage #8	04h	3Ah		
23	DR6	VIF volume liter	93h	E4h	# 3	
24	DR6	orth. VIFE, compact profile without registers	1Fh	24h		
25	DR6	LVAR length of profile (2+11*3 = 35 Bytes)	23h	27h		
26	DR6	Spacing control: signed diff., month, 6 digit BCD	FBh	CDh		
27	DR6	Spacing value: month, acc. to Annex I table I.9	FEh	A9h		
28	DR6	Value (LSB)	60h	DBh		
29	DR6	Value n-11 (February)	26h	24h		
30	DR6	Value (MSB)	00h	07h		
31	DR6	Value (LSB)	39h	FAh		
32	DR6	Value n-10 (March)	39h	81h	#3	APL

33	DR6	Value (MSB)	00h	31h	
34	DR6	Value (LSB)	34h	EFh	
35	DR6	Value n-9 (April)	31h	B2h	
36	DR6	Value (MSB)	00h	25h	
37	DR6	Value (LSB)	68h	97h	
38	DR6	Value n-8 (May)	34h	98h	
39	DR6	Value (MSB)	00h	E2h	# 4
40	DR6	Value (LSB)	10h	B7h	
41	DR6	Value n-7 (June)	42h	9Bh	
42	DR6	Value (MSB)	00h	AAh	
43	DR6	Value (LSB)	78h	D1h	
44	Checksum			31	DLL
45	Stop	Stop byte		16h	

N.4.5 Last fragment

The clear More Fragment Bit indicates the last Fragment.

REQ-UD2 (wM-Bus - Fragment 3)

Byte No		OMS M-Bus frame	GW -> MTR	Layer
	Field Name	Content	Bytes [hex]	
			plain	
1	Start	Start byte	10h	DLL
2	C Field	Respond user data	7Bh	
3	A Field	Addressing by secondary address	FDh	
4	Checksum		78h	
5	Stop	Stop byte	16h	

RSP-UD (M-Bus - Fragment3)

Byte No		OMS M-Bus frame (last fragment)	MTR->GW		Layer		
	Field Name	Content	Bytes [hex]	Bytes [hex]			
			plain	AES coded			
1	Start	Start byte		68h	DLL		
2	L Field	Length of data (33 bytes)		21h			
3	L Field	Length of data (33 bytes)		21h			
4	Start	Start byte		68h			
5	C Field	Respond user data		08h			
6	A Field	Addressing by secondary address		03h			
7	CI Field	AFL		90h	AFL		
8	AFLL	AFL Length Field		02h			
9	FCL	FID, Fragment-ID		03h			
10	FCL	MF=0, MCLP=0, MLP=0, MCRP=0, MACP=0		00h			
11	DR6	Value n-6 (July)	31h	AFh	# 4	APL	
12	DR6	Value (MSB)	00h	89h			
13	DR6	Value (LSB)	10h	B7h			
14	DR6	Value n-5 (August)	54h	50h			
15	DR6	Value (MSB)	00h	6Fh			
16	DR6	Value (LSB)	30h	EBh			
17	DR6	Value n-4 (September)	18h	16h			
18	DR6	Value (MSB)	00h	C2h			
19	DR6	Value (LSB)	86h	2Bh			
20	DR6	Value n-3 (October)	19h	15h			
21	DR6	Value (MSB)	00h	1Bh			
22	DR6	Value (LSB)	64h	35h	# 5		
23	DR6	Value n-2 (November)	24h	37h			
24	DR6	Value (MSB)	00h	FAh			
25	DR6	Value (LSB)	03h	27h			
26	DR6	Value n-1 (December)	41h	2Dh			
27	DR6	Value (MSB)	00h	55h			
28	DR7	DIF 16bit	02h	22h			
29	DR7	VIF from FD table	FDh	75h	#5	APL	

30	DR7	VIFE error flags, device specific	17h	62h	
31	DR7	Value error flags byte A	00h	C6h	
32	DR7	Value error flags byte B	00h	3Fh	
33	Dummy	Idle filler	2Fh	6Ch	
34	Dummy	Idle filler	2Fh	40h	
35	Dummy	Idle filler	2Fh	83h	
36	Dummy	Idle filler	2Fh	83h	
37	Dummy	Idle filler	2Fh	EBh	
38	Checksum			16h	DLL
39	Stop	Stop byte		16h	

N.5 Heat Cost Allocator

N.5.1 Input parameters

This example shows an asynchronous transmission of a heat cost allocator with an external unidirectional radio adapter. A presence transmission is done using ACC-NR. In the following SND-NR the application layer is partially encrypted only using Security profile A. This device signals an Low Power alert by the Status-Field.

Example for Heat cost allocator with RF-Adapter	
Medium	Heat cost allocation
Manufacturer	QDS
Ident number of Meter (HCA)	55667788
Version	85
Status (Low Power/Battery low)	4
Current cunsumption value	1234 HCA units
Due date	30.04.2007
Consumption at due date	23456 HCA units
Customer Location	12345678

RF adapter	
Medium/device type	55
Manufacturer	QDS
Ident number of RF-Adapter	11223344
Version	85

AES Key according to FIPS 197 (see 9.1):
= manu. spec. at least 8 bytes unique for each meter
= 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

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

N.5.2 wM-Bus Example with ACC-NR

Example for Heat cost allocator with RF-Adapter	
Medium	Heat cost allocation
Manufacturer	QDS
Ident number of Meter (HCA)	55667788
Version	85
Status (Low Power/Battery low)	4

RF adapter	
Medium/device type	55
Manufacturer	QDS
Ident number of RF-Adapter	11223344
Version	85

ACC-NR (wM-Bus)

		OMS wM-Bus frame	HCA -> GW	Layer
Byte No	Field Name	Content	Bytes [hex]	
			plain	
1	L Field	Length of data (25 bytes)	19h	Data Link Layer (DLL)
2	C Field	Access - No Reply	47h	
3	M Field	Manufacturer code	93h	
4	M Field	Manufacturer code	44h	
5	A Field	Ident No LSB (BCD)	44h	
6	A Field	Ident No (BCD)	33h	
7	A Field	Ident No (BCD) (= 11223344)	22h	
8	A Field	Ident No MSB (BCD)	11h	
9	A Field	Version (or Generation number)	55h	
10	A Field	Device type (RF-Adapter)	37h	
11	CRC 1		35h	
12	CRC 1		72h	
13	CI Field	Extended Link Layer (short)	8Ch	ELL
14	CC Field	Communication Control (unidir. sync.)	20h	
15	Access No.	ELL-Access Counter of Meter	75h	
16	CI Field	8Bh (long header)	8Bh	Transport Layer (TPL)
17	Meter-ID	Ident No LSB (BCD)	88h	
18	Meter-ID	Ident No (BCD)	77h	
19	Meter-ID	Ident No (BCD) (= 55667788)	66h	
20	Meter-ID	Ident No MSB (BCD)	55h	
21	Meter-Man.	Meter Manufacturer code	93h	
22	Meter-Man.	Meter Manufacturer code	44h	
23	Meter-Vers.	Version (or Generation number)	55h	
24	Meter-Med.	Device type (Medium=HCA)	08h	
25	Access No.	Access Number of Meter	FFh	
26	Status	Meter state (Low power)	04h	
27	Config Field	0000CCRHb (no encryption)	00h	
28	Config Field	BASMMMMMb	00h	
29	CRC 2		13h	DLL
30	CRC 2		93h	

N.5.3 wM-Bus Example with partial encryption

SND-NR (wM-Bus)

Byte No	Field Name	OMS wM-Bus frame Content	Heat cost allocator example Bytes [hex] plain	Bytes [hex] AES coded	Layer	
1	L Field	Length of data (48 bytes)		30h	Data Link Layer (DLL)	
2	C Field	Send - No Reply		44h		
3	M Field	Manufacturer code		93h		
4	M Field	Manufacturer code		44h		
5	A Field	Ident No LSB (BCD)		44h		
6	A Field	Ident No (BCD)		33h		
7	A Field	Ident No (BCD) (= 11223344)		22h		
8	A Field	Ident No MSB (BCD)		11h		
9	A Field	Version (or Generation number)		55h		
10	A Field	Device type (RF-Adapter)		37h		
11	CRC 1			A3h		
12	CRC 1			52h		
13	CI Field	Extended Link Layer (short)		8Ch	ELL	
14	CC Field	Communication Control (unidir. async.)		00h		
15	Access No.	ELL-Access Counter of Meter		75h		
16	CI Field	72h (long header)		72h	Transport Layer (TPL)	
17	Meter-ID	Ident No LSB (BCD)		88h		
18	Meter-ID	Ident No (BCD)		77h		
19	Meter-ID	Ident No (BCD) (= 55667788)		66h		
20	Meter-ID	Ident No MSB (BCD)		55h		
21	Meter-Man.	Meter Manufacturer code		93h		
22	Meter-Man.	Meter Manufacturer code		44h		
23	Meter-Vers.	Version (or Generation number)		55h		
24	Meter-Med.	Device type (Medium=HCA)		08h		
25	Access No.	Access Number of Meter		00h		
26	Status	Meter state (Low power)		04h		
27	Config Field	NNNNCCRHb (1 encr. block)		10h		
28	Config Field	BASMMMMMb (AES)		05h		
29	CRC 2			1Bh	DLL	
30	CRC 2			2Fh		
31	AES-Verify	Encryption verification	2Fh	00h	# 1	
32	AES-Verify	Encryption verification	2Fh	DFh		
33	DR1	DIF (6 digit BCD)	0Bh	E2h	# 1	Application Layer (APL)
34	DR1	VIF (HCA-units)	6Eh	A7h		
35	DR1	Value LSB	34h	82h		
36	DR1	Value (= 001234 HCA-Units)	12h	14h		
37	DR1	Value MSB	00h	6Dh		
38	DR2	DIF (Data type G, StorageNo 1)	42h	15h		
39	DR2	VIF (Date)	6Ch	13h		
40	DR2	Value LSB	FEh	58h		
41	DR2	Value MSB (= 30.04.2007)	04h	1Ch		
42	DR3	DIF (6 digit BCD, StorageNo 1)	4Bh	D2h		
43	DR3	VIF (HCA-units)	6Eh	F8h		
44	DR3	Value LSB	56h	3Fh		

45	DR3	Value (= 023456 HCA-Units)	34h	39h	#1	APL
46	DR3	Value MSB	02h	04h		
47	CRC 3			D7h	DLL	
48	CRC 3			57h		
49	DR4	DIF (8 digit BCD)	0Ch	0Ch	APL	
50	DR4	VIF (Extension Table FDh)	FDh	FDh		
51	DR4	VIFE (Customer Location)	10h	10h		
52	DR4	Value LSB	78h	78h		
53	DR4	Value (Location ID)	56h	56h		
54	DR4	Value	34h	34h		
55	DR4	Value MSB	12h	12h		
56	CRC 4			FBh	DLL	
57	CRC 4			35h		

SND-NR (wM-Bus)

		OMS wM-Bus frame	Heat cost allocator example		Layer
Byte No	Field Name	Content	Bytes [hex]	Bytes [hex]	
			plain	AES coded	
1	L Field	Length of data (48 bytes)		30h	Data Link Layer (DLL)
2	C Field	Send - No Reply		44h	
3	M Field	Manufacturer code		93h	
4	M Field	Manufacturer code		44h	
5	A Field	Ident No LSB (BCD)		44h	
6	A Field	Ident No (BCD)		33h	
7	A Field	Ident No (BCD) (= 11223344)		22h	
8	A Field	Ident No MSB (BCD)		11h	
9	A Field	Version (or Generation number)		55h	
10	A Field	Device type (RF-Adapter)		37h	
11	CRC 1			A3h	
12	CRC 1			52h	
13	CI Field	Extended Link Layer (short)		8Ch	ELL
14	CC Field	Communication Control (unidir. async.)		00h	
15	Access No.	ELL-Access Counter of Meter		75h	
16	CI Field	72h (long header)		72h	Transport Layer (TPL)
17	Meter-ID	Ident No LSB (BCD)		88h	
18	Meter-ID	Ident No (BCD)		77h	
19	Meter-ID	Ident No (BCD) (= 55667788)		66h	
20	Meter-ID	Ident No MSB (BCD)		55h	
21	Meter-Man.	Meter Manufacturer code		93h	
22	Meter-Man.	Meter Manufacturer code		44h	
23	Meter-Vers.	Version (or Generation number)		55h	
24	Meter-Med.	Device type (Medium=HCA)		08h	
25	Access No.	Access Number of Meter		00h	
26	Status	Meter state (Low power)		04h	
27	Config Field	NNNNCCRHb (1 encr. block)		10h	
28	Config Field	BASMMMMMb (AES)		05h	
29	CRC 2			1Bh	DLL
30	CRC 2			2Fh	
31	AES-Verify	Encryption verification	2Fh	00h	# 1
32	AES-Verify	Encryption verification	2Fh	DFh	

33	DR1	DIF (6 digit BCD)	0Bh	E2h	# 1	Application Layer (APL)
34	DR1	VIF (HCA-units)	6Eh	A7h		
35	DR1	Value LSB	34h	82h		
36	DR1	Value (= 001234 HCA-Units)	12h	14h		
37	DR1	Value MSB	00h	6Dh		
38	DR2	DIF (Data type G, StorageNo 1)	42h	15h		
39	DR2	VIF (Date)	6Ch	13h		
40	DR2	Value LSB	FEh	58h		
41	DR2	Value MSB (= 30.04.2007)	04h	1Ch		
42	DR3	DIF (6 digit BCD, StorageNo 1)	4Bh	D2h		
43	DR3	VIF (HCA-units)	6Eh	F8h		
44	DR3	Value LSB	56h	3Fh		
45	DR3	Value (= 023456 HCA-Units)	34h	39h	#1	APL
46	DR3	Value MSB	02h	04h		
47	CRC 3			D7h		DLL
48	CRC 3			57h		
49	DR4	DIF (8 digit BCD)	0Ch	0Ch		APL
50	DR4	VIF (Extension Table FDh)	FDh	FDh		
51	DR4	VIFE (Customer Location)	10h	10h		
52	DR4	Value LSB	78h	78h		
53	DR4	Value (Location ID)	56h	56h		
54	DR4	Value	34h	34h		

N.5.4 M-Bus Example with partial encryption

RSP-UD (M-Bus with Encryption)

Byte No	Field Name	OMS M-Bus frame Content	HCA example Bytes [hex] plain	HCA example Bytes [hex] AES coded	Layer
1	Start	Start byte		68h	Data Link Layer (DLL)
2	L Field	Length of data (44bytes)		2Ch	
3	L Field	Length of data (44 bytes)		2Ch	
4	Start	Start byte		68h	
5	C Field	Respond user data		08h	
6	A-Field	Secondary addressing mode		FDh	
7	CI Field	72h (long header)		72h	Transport Layer (TPL)
8	Ident.Nr.	Ident No LSB (BCD)		88h	
9	Ident.Nr.	Ident No (BCD)		77h	
10	Ident.Nr.	Ident No (BCD) (=55667788)		66h	
11	Ident.Nr.	Ident No MSB (BCD)		55h	
12	Manufr	Manufacturer code		93h	
13	Manufr	Manufacturer code		44h	
14	Version	Version (or Generation number)		55h	
15	Device type	Device type (Medium=HCA)		08h	
16	Access No.	Access Number of Meter		00h	
17	Status	Meter state (Low power)		04h	
18	Config Field	NNNNCCRHb (1 encr. block)		10h	
19	Config Field	BASMMMMMb (AES)		05h	
20	AES-Verify	Encryption verification	2Fh	00h	
21	AES-Verify	Encryption verification	2Fh	DFh	
22	DR1	DIF (6 digit BCD)	0Bh	E2h	Application Layer (APL)
23	DR1	VIF (HCA-units)	6Eh	A7h	
24	DR1	Value LSB	34h	82h	
25	DR1	Value (= 001234 HCA-Units)	12h	14h	
26	DR1	Value MSB	00h	6Dh	
27	DR2	DIF (Data type G, StorageNo 1)	42h	15h	
28	DR2	VIF (Date)	6Ch	13h	
29	DR2	Value LSB	FEh	58h	
30	DR2	Value MSB (= 30.04.2007)	04h	1Ch	
31	DR3	DIF (6 digit BCD, StorageNo 1)	4Bh	D2h	
32	DR3	VIF (HCA-units)	6Eh	F8h	
33	DR3	Value LSB	56h	3Fh	
34	DR3	Value (= 023456 HCA-Units)	34h	39h	
35	DR3	Value MSB	02h	04h	
36	DR4	DIF (8 digit BCD)	0Ch	0Ch	
37	DR4	VIF (Extension Table FDh)	FDh	FDh	
38	DR4	VIFE (Customer Location)	10h	10h	
39	DR4	Value LSB	78h	78h	
40	DR4	Value (Location ID)	56h	56h	
41	DR4	Value	34h	34h	
42	DR4	Value MSB	12h	12h	
43	DR5	DIF (8 digit BCD)	0Ch	0Ch	

44	DR5	VIF (Fabrication number)	78h	78h	APL
45	DR5	Value LSB	44h	44h	
46	DR5	Value (Ident-Nr of Adapter)	33h	33h	
47	DR5	Value	22h	22h	
48	DR5	Value MSB	11h	11h	
49	Checksum			26h	DLL
50	Stop	Stop byte		16h	

N.6 Installation Procedure with a Special Installation Datagram

This example shows a special transmission of a Gas meter with Request for installation. The Gateway confirms this request. Note that the GW sends however an additional SND-NKE a few seconds after the CNF-IR.

5

GW example	
Medium	Communication Controller
Manufacturer	XYZ (633A)
Ident number	33445566
Version	10 (e.g. V 1.0)

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

AES Key According to FIPS 197 (see 9.1):
= manu. spec. at least 8 bytes unique for each meter
= 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 11

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

SND-IR (wM-Bus)

Byte No	Field Name	Content	Gas meter -> GW: Bytes [hex] plain	Gas meter -> GW: Bytes [hex] AES coded	Layer
1	L Field	Length of data (81 bytes)		51h	Data Link Layer (DLL)
2	C Field	Send - Installation Request		46h	
3	M Field	Manufacturer code		93h	
4	M Field	Manufacturer code		15h	
5	A Field	Ident No LSB (BCD)		78h	
6	A Field	Ident No (BCD)		56h	
7	A Field	Ident No (BCD) (=12345678)		34h	
8	A Field	Ident No MSB (BCD)		12h	
9	A Field	Version (or Generation number)		33h	
10	A Field	Device type (Medium=Gas)		03h	
11	CRC 1			EFh	
12	CRC 1			B5h	
13	CI Field	Extended Link Layer (short)		8Ch	ELL
14	CC Field	Communication Control (bidir., RX off)		80h	
15	Access No.	Access Number of Meter		45h	
16	CI Field	7Ah (short header)		7Ah	Transport Layer (TPL)
17	Access No.	Access Number of Meter		01h	
18	Status	Meter state		00h	
19	Config Field	NNNNCCRHb (4 encr. blocks, static tlg.)		48h	
20	Config Field	BASMMMMMb (AES)		05h	
21	AES-Verify	Encryption verification	2Fh	D2h	
22	AES-Verify	Encryption verification	2Fh	B7h	
23	DR1	DIF (Variable length)	0Dh	0Bh	APL # 1
24	DR1	VIF (Extension)	FDh	3Fh	
25	DR1	VIFE (Version)	0Ch	BCh	
26	DR1	LVAR (= 4 byte text string)	04h	1Ah	
27	DR1	Value (LSB)	34h	15h	
28	DR1	Value (= BKG4)	47h	80h	
29	CRC 2			**C8h**	DLL
30	CRC 2			**5Eh**	
31	DR1	Value	4Bh	D7h	Application Layer (APL) # 1
32	DR1	Value (MSB)	42h	9Bh	
33	DR2	DIF (**4 digit BCD**)	0**A**h	92h	
34	DR2	VIF (Extension)	FDh	CAh	
35	DR2	VIFE (Hardware version)	0Dh	A1h	
36	DR2	Value LSB (=1.5)	05h	D9h	
37	DR2	Value MSB	01h	53h	
38	DR3	DIF (**4 digit BCD**)	0**A**h	41h	
39	DR3	VIF (Extension)	FDh	B6h	Application Layer (APL) # 2
40	DR3	VIFE (Metrology Firmware version)	0Eh	09h	
41	DR3	Value LSB (= 1.1)	01h	EFh	
42	DR3	Value MSB	01h	60h	
43	DR4	DIF (**4 digit BCD**)	0**A**h	3Ah	
44	DR4	VIF (Extension)	FDh	D3h	
45	DR4	VIFE (Other firmware version)	0Fh	62h	

46	DR4	Value LSB (= 1.0)	00h	94h		
47	CRC 3			85h	DLL	
48	CRC 3			3Ah		
49	DR4	Value MSB	01h	72h	# 2	Application Layer (APL)
50	DR5	DIF (Variable length)	0Dh	B2h		
51	DR5	VIF (Extension)	FDh	06h		
52	DR5	VIFE (customer location)	10h	7Dh		
53	DR5	LVAR (=33 byte text string)	21h	26h		
54	DR5	Value LSB	38h	BDh		
55	DR5	Value (= 00000000000012345678)	37h	2Bh		
56	DR5	Value	36h	5Fh		
57	DR5	Value	35h	DDh	# 3	
58	DR5	Value	34h	C2h		
59	DR5	Value	33h	37h		
60	DR5	Value	32h	4Dh		
61	DR5	Value	31h	29h		
62	DR5	Value	30h	D0h		
63	DR5	Value	30h	CDh		
64	DR5	Value	30h	08h		
65	CRC 4			ABh	DLL	
66	CRC 4			48h		
67	DR5	Value	30h	58h	# 3	Application Layer (APL)
68	DR5	Value	30h	C5h		
69	DR5	Value	30h	61h		
70	DR5	Value	30h	4Eh		
71	DR5	Value	30h	8Bh		
72	DR5	Value	30h	56h		
73	DR5	Value	30h	E6h		
74	DR5	Value	30h	C2h		
75	DR5	Value	30h	17h	# 4	
76	DR5	Value (= 49074)	34h	59h		
77	DR5	Value	37h	62h		
78	DR5	Value	30h	DBh		
79	DR5	Value	39h	0Fh		
80	DR5	Value	34h	01h		
81	DR5	Value (= 123456)	36h	AAh		
82	DR5	Value	35h	2Ah		
83	CRC 5			62h	DLL	
84	CRC 5			E1h		
85	DR5	Value	34h	A7h	# 4	APL
86	DR5	Value	33h	B1h		
87	DR5	Value	32h	2Eh		
88	DR5	Value	31h	E4h		
89	DR5	Value (= DE)	45h	B5h		
90	DR5	Value MSB	44h	F6h		
91	Dummy	Fill Byte due to AES	2Fh	3Fh		
92	Dummy	Fill Byte due to AES	2Fh	44h		
93	CRC 6			05h	DLL	
94	CRC 6			69h		

CNF-IR (wM-Bus)

Byte No	Field Name	OMS wM-Bus frame Content	GW -> Gas meter Bytes [hex] plain	Layer
1	L Field	Length of data (25 bytes)	19h	Data Link Layer (DLL)
2	C Field	Confirm - Installation Request	06h	
3	M Field	Manufacturer code	3Ah	
4	M Field	Manufacturer code	63h	
5	A Field	Ident No LSB (BCD)	66h	
6	A Field	Ident No (BCD)	55h	
7	A Field	Ident No (BCD) (=33445566)	44h	
8	A Field	Ident No MSB (BCD)	33h	
9	A Field	Version (or Generation number)	0Ah	
10	A Field	Device type (Medium=COM)	31h	
11	CRC 1		90h	
12	CRC 1		72h	
13	CI Field	Extended Link Layer (short)	8Ch	ELL
14	CC Field	Communication Control (bidir., RX on)	84h	
15	Access No.	Access Number of Meter	45h	
16	CI Field	80h means 12 byte header	80h	Transport Layer (TPL)
17	Ident.Nr.	Ident No LSB (BCD)	78h	
18	Ident.Nr.	Ident No (BCD)	56h	
19	Ident.Nr.	Ident No (BCD) (=12345678)	34h	
20	Ident.Nr.	Ident No MSB (BCD)	12h	
21	Manufr	Manufacturer code	93h	
22	Manufr	Manufacturer code	15h	
23	Version	Version (or Generation number)	33h	
24	Device type	Device type (Medium=Gas)	03h	
25	Access No.	Access Number of Meter	01h	
26	Status	GW state cont. recept. level (-80dBm)	19h	
27	Config Field	0000CCRHb	00h	
28	Config Field	BASMMMMMb (no encr.)	00h	
29	CRC 2		93h	DLL
30	CRC 2		FDh	

N.7 Send a Command

N.7.1 Input parameters

A SND-UD is applied to transport a command to a meter or actuator. When C-Field 53h or 73h is applied the meter will acknowledge a successful reception of the command. The bit "application error" in the Status Byte of the acknowledge datagram indicates an application error during the command execution.

GW example	
Medium/device type	Communication Controller
Manufacturer	HYD
Ident number	90123456
Version	8

RF adapter example	
Medium/device type	Radio converter
Manufacturer	HYD
Ident number RF adapter	43886102
Version	41

Example of mechanical water meter	
Medium/device type	Water meter
Manufacturer	QDS
Ident number water meter	92752244
Version	-

AES Key According to FIPS 197 (see 9.1):
= manu. spec. at least 8 bytes unique for each meter
= 82 B0 55 11 91 F5 1D 66 EF CD AB 89 67 45 23 01

AES CBC Initial Vector according to FIPS 197 (LSB first):
= M Field + A Field + 8 bytes Acces No
= 93 44 44 22 75 92 00 07 7D 7D 7D 7D 7D 7D 7D 7D

N.7.2 Command Adjust Clock Time by Gateway with Security profile A

SND-UD Adjust Clock Time (wM-Bus)

Byte No	Field Name	OMS wM-Bus frame Content	GW -> water meter Bytes [hex] plain	GW -> water meter Bytes [hex] AES coded	Layer	
1	L Field	Length of data (41 bytes)		29h	Data Link Layer (DLL)	
2	C Field	Send user data		53h		
3	M Field	Manufacturer code		24h		
4	M Field	Manufacturer code		23h		
5	A Field	Ident No LSB (BCD)		56h		
6	A Field	Ident No (BCD)		34h		
7	A Field	Ident No (BCD)		12h		
8	A Field	Ident No MSB (BCD) of GW		90h		
9	A Field	Version (or Generation number)		08h		
10	A Field	Device type (Medium=COM)		31h		
11	CRC 1			88h		
12	CRC 1			8Ah		
13	CI Field	Extended Link Layer (short)		8Ch	ELL	
14	CC Field	Communication Control (bidir., RX on)		84h		
15	Access No.	Access Number of GW		51h		
16	CI Field	Special CI to add/subtract time offset		6Dh	Transport Layer (TPL)	
17	Ident.Nr.	Ident No LSB (BCD)		44h		
18	Ident.Nr.	Ident No (BCD)		22h		
19	Ident.Nr.	Ident No (BCD)		75h		
20	Ident.Nr.	Ident No MSB (BCD) of meter		92h		
21	Manufr	Manufacturer code		93h		
22	Manufr	Manufacturer code		44h		
23	Version	Version (or Generation number)		00h		
24	Device type	Device type (Medium = Water)		07h		
25	Access No.	Access Number of GW		7Dh		
26	Status	GW state (no RSSI level available)		00h		
27	Config Field	NNNNCCRHb (1 encr. block)		10h		
28	Config Field	BASMMMMMb (AES)		05h		
29	CRC 2			81h	DLL	
30	CRC 2			98h		
31	AES-Verify	Encryption verification	2Fh	9Eh		TPL
32	AES-Verify	Encryption verification	2Fh	D8h		
33	TC-Field	Add time difference	01h	2Ah	# 1	Application Layer (APL)
34	Time	Value format J, LSB	32h	B2h		
35	Time	Value (add 1 minute, 50 seconds)	01h	33h		
36	Time	Value MSB	00h	D1h		
37	Reserved	Reserved, set to 0	00h	A2h		
38	Reserved	Reserved, set to 0	00h	A8h		
39	Reserved	Reserved, set to 0	00h	0Bh		
40	Reserved	Reserved, set to 0	00h	FFh		
41	Reserved	Reserved, set to 0	00h	D3h		
42	Reserved	Reserved, set to 0	00h	B7h		
43	CMD-Verify	Command verification	2Fh	B6h		
44	CMD-Verify	Command verification	2Fh	A9h		

45	CMD-Verify	Command verification	2Fh	08h	
46	CMD-Verify	Command verification	2Fh	D7h	
47	CRC 3			C5h	DLL
48	CRC 3			AAh	

ACK (wM-Bus)

		OMS wM-Bus frame	water meter -> GW	Layer
Byte No	Field Name	Content	Bytes [hex]	
			plain	
1	L Field	Length of data (25 bytes)	19h	Data Link Layer (DLL)
2	C Field	Acknowledge	00h	
3	M Field	Manufacturer code	24h	
4	M Field	Manufacturer code	23h	
5	A Field	Ident No LSB (BCD)	02h	
6	A Field	Ident No (BCD)	61h	
7	A Field	Ident No (BCD)	88h	
8	A Field	Ident No MSB (BCD) of RF-Adapter	43h	
9	A Field	Version (or Generation number)	29h	
10	A Field	Device type (Medium=Water)	07h	
11	CRC 1		77h	
12	CRC 1		83h	
13	CI Field	Extended Link Layer (short)	8Ch	ELL
14	CC Field	Communication Control (bidir, RX off)	80h	
15	Access No.	Access Number of GW	51h	
16	CI Field	8Bh means long header	8Bh	Transport Layer (TPL)
17	Ident.Nr.	Ident No LSB (BCD)	44h	
18	Ident.Nr.	Ident No (BCD)	22h	
19	Ident.Nr.	Ident No (BCD)	75h	
20	Ident.Nr.	Ident No MSB (BCD) of meter	92h	
21	Manufr	Manufacturer code	93h	
22	Manufr	Manufacturer code	44h	
23	Version	Version (or Generation number)	00h	
24	Device type	Device type (Medium=Water)	07h	
25	Access No.	Access Number of GW	7Dh	
26	Status	Meter state	02h	
27	Config Field	0000CCRHb	00h	
28	Config Field	BASMMMMMb (no encr.)	00h	
29	CRC 2		A6h	DLL
30	CRC 2		B5h	

The Status byte indicates an application error, because the applied range for the command time adjustment is out of range (see OMS-S2, Annex M, OMS-UC-04a). The meter will respond with an application error 15_h to the next REQ-UD2.

5

N.8 Request of the Selected Data

A REQ-UD2 is used either to request the standard meter consumption data or to read responses of a command or prove successful execution of a command. After a command the RSP-UD may consist of either the expected answer to that read command (e.g. “get valve state”) or the standard answer if a write command like “set new key” was applied or an “application error” if the execution of the command was not successful (e.g. using the wrong encryption key for this meter). An application error will be indicated in the Status Byte of the meter’s acknowledge datagram.

Example for GW	
Medium	Communication Controller
Manufacturer	TCH
Ident number	66778899
Version	12
Status (no error)	0
Meter-RSSI	-84 dBm

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

AES Key According to FIPS 197 (see 9.1):
= manu. spec. at least 8 bytes unique for each meter
= 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

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

This example shows a normal response and an “application error”, which is responded instead of expected data because the gateway applied a wrong CI-Field.

RSP-UD (wM-Bus)

Byte No		OMS wM-Bus frame	HCA -> GW		Layer	
	Field Name	Content	Bytes [hex]	Bytes [hex]		
			plain	AES coded		
1	L Field	Length of data (33 bytes)		21h	Data Link Layer (DLL)	
2	C Field	Respond user data		08h		
3	M Field	Manufacturer code		68h		
4	M Field	Manufacturer code		50h		
5	A Field	Ident No LSB (BCD)		78h		
6	A Field	Ident No (BCD)		56h		
7	A Field	Ident No (BCD) (=12345678)		34h		
8	A Field	Ident No MSB (BCD) of meter		12h		
9	A Field	Version (or Generation number)		8Fh		
10	A Field	Device type (Medium=HCA)		08h		
11	CRC 1			E4h		
12	CRC 1			F8h		
13	CI Field	Extended Link Layer (short)		8Ch	ELL	
14	CC Field	Communication Control (bidir.,RX off)		80h		
15	Access No.	Access Number of GW		15h		
16	CI Field	7Ah (short header)		7Ah	Transport Layer (TPL)	
17	Access No.	Access Number of GW		02h		
18	Status	Meter state		00h		
19	Config Field	NNNNCCRHb (1 encr. block)		10h		
20	Config Field	BASMMMMMb, (AES)		05h		
21	AES-Verify	Encryption verification	2Fh	FDh		
22	AES-Verify	Encryption verification	2Fh	26h		
23	DR1	DIF (24 bit binary, StorageNo 0)	03h	EFh	# 1	APL
24	DR1	VIF (HCA-units)	6Eh	68h		
25	DR1	Value LSB	39h	ACh		
26	DR1	Value (= 012345d = 003039h HCA-Units)	30h	F6h		
27	DR1	Value MSB	00h	5Bh		
28	DR2	DIF (16 bit binary, StorageNo 1)	42h	AEh		
29	CRC 2			39h	DLL	
30	CRC 2			F9h		
31	DR2	VIF (Date type G)	6Ch	02h	# 1	Application Layer
32	DR2	Value LSB	3Fh	8Bh		
33	DR2	Value MSB (= 31.12.2009)	1Ch	FDh		
34	DR3	DIF (24 bit binary, StorageNo 1)	43h	C1h		
35	DR3	VIF (HCA-units)	6Eh	88h		
36	DR3	Value LSB	A0h	D8h		
37	DR3	Value (= 023456 = 005BA0h HCA-Units)	5Bh	A9h		
38	DR3	Value MSB	00h	72h		
39	CRC 3			D8h	DLL	
40	CRC 3			DCh		

or alternatively …

RSP-UD (wM-Bus - Appl. Error)

Byte No		OMS wM-Bus frame	HCA -> GW	Layer
	Field Name	Content	Bytes [hex]	
			plain	
1	L Field	Length of data (18 bytes)	12h	Data Link Layer (DLL)
2	C Field	Respond user data	08h	
3	M Field	Manufacturer code	68h	
4	M Field	Manufacturer code	50h	
5	A Field	Ident No LSB (BCD)	78h	
6	A Field	Ident No (BCD)	56h	
7	A Field	Ident No (BCD) (=12345678)	34h	
8	A Field	Ident No MSB (BCD)	12h	
9	A Field	Version (or Generation number)	8Fh	
10	A Field	Device type (Medium=HCA)	08h	
11	CRC 1		96h	
12	CRC 1		89h	
13	CI Field	Extended Link Layer (short)	8Ch	ELL
14	CC Field	Communication Control (bidir.,RX off)	80h	
15	Access No.	Access Number of GW	15h	
16	CI Field	Application Error (short header)	6Eh	Transport Layer (TPL)
17	Access No.	Access Number of GW	02h	
18	Status	Meter state “any application error”	02h	
19	Config Field	0000CCRHb	00h	
20	Config Field	BASMMMMMb (no encryption)	00h	
21	Error Code	CI-Field not implemented	01h	APL
22	CRC 2		B5h	DLL
23	CRC 2		A3h	

N.9 Demand for Access

This Example shows a Meter sending a ACC-DMD Message. The gateway acknowledges this demand. Thereafter the gateway is in charge to request the reason of this access demand from the meter.

NOTE: This is the only bidirectional communication initiated by the meter.

GW example	
Medium/device type	Communication Controller
Manufacturer	XYZ (633A)
Ident number	12345678
Version	2

water meter with RF adapter example	
Medium/device type	Water
Manufacturer	ZYX (6B38)
Ident number water meter	38546816
Version	25

RF adapter example	
Medium/device type	Radio converter
Manufacturer	WEP (5CB0h)
Ident number RF-Adapter	08154711
Version	17

ACC-DMD (wM-Bus)

Byte No	Field Name	Content	Bytes [hex] plain	Layer
		OMS wM-Bus frame	water meter -> GW	
1	L Field	Length of data (25 bytes)	19h	Data Link Layer (DLL)
2	C Field	Access demand to master	48h	
3	M Field	Manufacturer code	B0h	
4	M Field	Manufacturer code	5Ch	
5	A Field	Ident No LSB (BCD)	11h	
6	A Field	Ident No (BCD)	47h	
7	A Field	Ident No (BCD)	15h	
8	A Field	Ident No MSB (BCD) of RF-Adapter	08h	
9	A Field	Version (or Generation number)	11h	
10	A Field	Device type (Medium=RF-Adapter)	37h	
11	CRC 1		B3h	
12	CRC 1		65h	
13	CI Field	Extended Link Layer (2 bytes)	8Ch	ELL
14	CC Field	Communication Control (bidir. sync.)	A0h	
15	Access No.	Access Number of Meter	51h	
16	CI Field	CI-Field Pure Transport Layer	8Bh	Transport Layer (TPL)
17	Ident.Nr.	Ident No LSB (BCD)	16h	
18	Ident.Nr.	Ident No (BCD)	68h	
19	Ident.Nr.	Ident No (BCD)	54h	
20	Ident.Nr.	Ident No MSB (BCD) of meter	38h	
21	Manufr	Manufacturer code	38h	
22	Manufr	Manufacturer code	6Bh	
23	Version	Version (or Generation number)	19h	
24	Device type	Device type (Medium = Water)	07h	
25	Access No.	Access Number of Meter	51h	
26	Status	Meter state	00h	
27	Config Field	0000CCRHb	00h	
28	Config Field	BASMMMMMb	00h	
29	CRC 2		0Eh	DLL
30	CRC 2		ACh	

ACK (wM-Bus)

Byte No	Field Name	Content	Bytes [hex] plain	Layer
		OMS wM-Bus frame	GW -> water meter	
1	L Field	Length of data (25 bytes)	19h	Data Link Layer (DLL)
2	C Field	Acknowledge	00h	
3	M Field	Manufacturer code	3Ah	
4	M Field	Manufacturer code	63h	
5	A Field	Ident No LSB (BCD)	78h	
6	A Field	Ident No (BCD)	56h	
7	A Field	Ident No (BCD)	34h	
8	A Field	Ident No MSB (BCD) of GW	12h	
9	A Field	Version (or Generation number)	02h	
10	A Field	Device type (Medium=COM)	31h	
11	CRC 1		C2h	
12	CRC 1		BAh	
13	CI Field	Extended Link Layer (short)	8Ch	ELL
14	CC Field	Communication Control (bidir, RX off)	80h	
15	Access No.	Access Number of GW	51h	
16	CI Field	CI-Field Pure Transport Layer	80h	Transport Layer (TPL)
17	Ident.Nr.	Ident No LSB (BCD)	16h	
18	Ident.Nr.	Ident No (BCD)	68h	
19	Ident.Nr.	Ident No (BCD)	54h	
20	Ident.Nr.	Ident No MSB (BCD) of meter	38h	
21	Manufr	Manufacturer code	38h	
22	Manufr	Manufacturer code	6Bh	
23	Version	Version (or Generation number)	19h	
24	Device type	Device type (Medium=Water)	07h	
25	Access No.	Access Number of GW	51h	
26	Status	GW-state RSSI level (-84 dBm)	17h	
27	Config Field	0000CCRHb	00h	
28	Config Field	BASMMMMMb (no encr.)	00h	
29	CRC 2		55h	DLL
30	CRC 2		37h	

N.10 Reset of the Link by a SND-NKE

If the gateway intends to finish communication it sends a SND-NKE as last. The meter/actuator does not responds to this SND-NKE.

The SND-NKE is also applied by the gateway to signal the capability to receive this meter. The reception level allows an estimation of the link quality.

GW example	
Medium	Communication Controller
Manufacturer	XYZ (633A)
Ident number	66778899
Version	12
Meter-RSSI	-66 dBm
Access number	03

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

SND-NKE (wM-Bus)

Byte No	Field Name	Content	Bytes [hex] plain	Layer
		OMS wM-Bus frame	GW -> cooling meter	
1	L Field	Length of data (25 bytes)	19h	Data Link Layer (DLL)
2	C Field	Request user data class 2 (5Bh or 7Bh)	40h	
3	M Field	Manufacturer code	3Ah	
4	M Field	Manufacturer code	63h	
5	A Field	Ident No LSB (BCD)	99h	
6	A Field	Ident No (BCD)	88h	
7	A Field	Ident No (BCD) (=66778899)	77h	
8	A Field	Ident No MSB (BCD) of GW	66h	
9	A Field	Version (or Generation number)	0Ch	
10	A Field	Device type (Medium=COM)	31h	
11	CRC 1		9Bh	
12	CRC 1		B7h	
13	CI Field	Extended Link Layer (short)	8Ch	ELL
14	CC Field	Communication Control (bidir., RX on)	84h	
15	Access No.	ELL-Access Counter of GW	32h	
16	CI Field	GW -> Meter (long header)	80h	Transport Layer (TPL)
17	Ident.Nr.	Ident No LSB (BCD)	44h	
18	Ident.Nr.	Ident No (BCD)	33h	
19	Ident.Nr.	Ident No (BCD) (=11223344)	22h	
20	Ident.Nr.	Ident No MSB (BCD)	11h	
21	Manufr	Manufacturer code	93h	
22	Manufr	Manufacturer code	44h	
23	Version	Version (or Generation number)	10h	
24	Device type	Device type (Medium=Cool_outlet)	0Ah	
25	Access No.	Access Number of GW	03h	
26	Status	GW State RSSI level (-66dBm)	20h	
27	Config Field	0000CCRHb	00h	
28	Config Field	BASMMMMMb, (no encr.)	00h	
29	CRC 2		DAh	DLL
30	CRC 2		8Eh	

N.11 Breaker (short ELL+AFL+ASP)

N.11.1 SND-NR (wM-Bus)

Breaker example	
Medium	Breaker
Manufacturer	XYZ (633A)
Ident number	12345678
Version	85
Current state	connected (01h)

GW example	
Medium/device type	Communication Controller
Manufacturer	XYZ (633A)
Ident number	87654321
Version	8

ToDo:
1. Calculate Session Keys
2. Encrypt Message using Kenc
3. Calculate MAC using Kmac
4. Calculate CRCs

Individual Master Key Mk (see 9.1):
= 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

Message Counter CM SND-NR (LSB first):
= B3 0A 00 00

Encryption Session Key Kenc SND-NR
= CMAC(Mk, 0x00 || MCR || IdentNo || padding) = CMAC(Mk,00||B3||0A||00||00||78||56||34||12 … ... ||07||07||07||07||07||07||07) = EC CF 39 D4 75 D7 30 B8 28 4F DF DC 19 95 D5 2F

MAC Session Key Kmac SND-NR
= CMAC(Mk, 0x01 || MCR || IdentNo || padding) = CMAC(Mk,01||B3||0A||00||00||78||56||34||12 … ... ||07||07||07||07||07||07||07) = C9 CD 19 FF 5A 9A AD 5A 6B BD A1 3B D2 C4 C7 AD

SND-NR (wM-Bus)

Byte No	Field Name	Content	Breaker example Bytes [hex] plain	Breaker example Bytes [hex] AES coded	Layer
1	L Field	Length of data (51 bytes)		33h	Data Link Layer (DLL)
2	C Field	Send - No Reply		44h	
3	M Field	Manufacturer code		3Ah	
4	M Field	Manufacturer code		63h	
5	A Field	Ident No LSB (BCD)		78h	
6	A Field	Ident No (BCD)		56h	
7	A Field	Ident No (BCD) (= 12345678)		34h	
8	A Field	Ident No MSB (BCD)		12h	
9	A Field	Version (or Generation number)		55h	
10	A Field	Device type (Breaker)		20h	
11	CRC 1			E4h	
12	CRC 1			C9h	
13	CI Field	Extended Link Layer (short)		8Ch	ELL
14	CC Field	Communication Control (bidi., RX on, Sync.)		A4h	
15	Access No.	ELL-Access Counter of actuator		E5h	
16	CI Field	Authentication and Fragmentation layer		90h	Authentication and Fragmentation Layer (AFL)
17	AFLL	AFL Length (all AFL bytes after AFLL)		0Fh	
18	FCL	Fragmentation Control Field (LSB)		00h	
19	FCL	Fragmentation Control Field (MSB)		2Ch	
20	MCL	Message Control Field		25h	
21	MCR	Message Counter CM (LSB)		B3h	
22	MCR	Message Counter CM		0Ah	
23	MCR	Message Counter CM (e.g. = 2739)		00h	
24	MCR	Message Counter CM (MSB)		00h	
25	MAC	AES-CMAC (MSB)		EDh	
26	MAC	AES-CMAC		17h	
27	MAC	AES-CMAC		23h	
28	MAC	AES-CMAC		68h	
29	CRC 2			E6h	DLL
30	CRC 2			B5h	
31	MAC	AES-CMAC		27h	AFL
32	MAC	AES-CMAC		CEh	
33	MAC	AES-CMAC		A2h	
34	MAC	AES-CMAC (LSB)		FFh	
35	CI Field	7Ah (short header)		7Ah	TPL
36	Access No.	TPL Access Counter of actuator		75h	
37	Status	Status		00h	
38	Config Field	NNNNPIIIb		10h	
39	Config Field	CCZMMMMMb		07h	
40	CFE	0VDDKKKKb		10h	
41	AES-Verify	Decryption verification	2Fh	B3h	
42	AES-Verify	Decryption verification	2Fh	8Ch	

43	DR1	DIF (8 bit integer)	01h	55h	# 1	APL
44	DR1	VIF (2nd Extension table)	FDh	00h		
45	DR1	VIFE (Remote control)	1Fh	99h		
46	DR1	Value (breaker conencted)	01h	33h		
47	CRC 3			A6h	DLL	
48	CRC 3			04h		
49	Dummy	Fill Byte due to AES	2Fh	41h	# 1	Application Layer (APL)
50	Dummy	Fill Byte due to AES	2Fh	B1h		
51	Dummy	Fill Byte due to AES	2Fh	23h		
52	Dummy	Fill Byte due to AES	2Fh	67h		
53	Dummy	Fill Byte due to AES	2Fh	4Fh		
54	Dummy	Fill Byte due to AES	2Fh	59h		
55	Dummy	Fill Byte due to AES	2Fh	38h		
56	Dummy	Fill Byte due to AES	2Fh	D2h		
57	Dummy	Fill Byte due to AES	2Fh	99h		
58	Dummy	Fill Byte due to AES	2Fh	33h		
59	CRC 4			08h	DLL	
60	CRC 4			13h		

N.11.2 SND-UD2 (wM-Bus)

Breaker example	
Medium	Breaker
Manufacturer	XYZ (633A)
Ident number	12345678
Version	85
Current state	connected (01h)

GW example	
Medium/device type	Communication Controller
Manufacturer	XYZ (633A)
Ident number	87654321
Version	8

ToDo:
1. Calculate Session Keys
2. Encrypt Message using Kenc
3. Calculate MAC using Kmac
4. Calculate CRCs

Individual Master Key Mk (see 9.1):
= 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

Message Counter CGW SND-UD2 (LSB first):
= F0 0A 00 00

Encryption Session Key Lenc SND-UD2
= CMAC(Mk, 0x10 || MCR || IdentNo || padding) = CMAC(Mk,10||F0||0A||00||00||78||56||34||12 … ... ||07||07||07||07||07||07||07) = C8 07 12 E7 20 02 5D B9 B4 B5 08 19 C2 44 50 35

MAC Session Key Lmac SND-UD2
= CMAC(Mk, 0x11 || MCR || IdentNo || padding) = CMAC(Mk,11||F0||0A||00||00||78||56||34||12 … ... ||07||07||07||07||07||07||07) = B6 85 94 D4 42 12 BB BB FD 99 05 CC 40 21 23 5B

Application security key for disconnection & reconnection: (Key ID: 20h / Key Version: 00h)
= 08 15 47 11 08 15 47 11 08 15 47 11 08 15 47 11

SND-UD2 (wM-Bus)

Byte No	Field Name	Content	GW -> Breaker Bytes [hex] plain	GW -> Breaker Bytes [hex] AES coded	Layer
1	L Field	Length of data (75 bytes)		4Bh	Data Link Layer (DLL)
2	C Field	Send - UserData2		43h	
3	M Field	Manufacturer code		3Ah	
4	M Field	Manufacturer code		63h	
5	A Field	Ident No LSB (BCD)		21h	
6	A Field	Ident No (BCD)		43h	
7	A Field	Ident No (BCD) (= 87654321)		65h	
8	A Field	Ident No MSB (BCD)		87h	
9	A Field	Version (or Generation number)		08h	
10	A Field	Device type (Medium=COM)		31h	
11	CRC 1			87h	
12	CRC 1			71h	
13	CI Field	Extended Link Layer (short)		8Ch	ELL
14	CC Field	Communication Control (bidir., RX on)		84h	
15	Access No.	Access Number of GW		23h	
16	CI Field	Authentication and Fragmentation layer		90h	Authentication and Fragmentation Layer (AFL)
17	AFLL	AFL Length (all AFL bytes after AFLL)		0Fh	
18	FCL	Fragmentation Control Field (LSB)		00h	
19	FCL	Fragmentation Control Field (MSB)		2Ch	
20	MCL	Message Control Field		25h	
21	MCR	Message Counter CGW (LSB)		F0h	
22	MCR	Message Counter CGW		0Ah	
23	MCR	Message Counter CGW (e.g. = 2800)		00h	
24	MCR	Message Counter CGW (MSB)		00h	
25	MAC	AES-CMAC (MSB)		87h	
26	MAC	AES-CMAC		E2h	
27	MAC	AES-CMAC		77h	
28	MAC	AES-CMAC		72h	
29	CRC 2			72h	DLL
30	CRC 2			44h	
31	MAC	AES-CMAC		2Eh	AFL
32	MAC	AES-CMAC		67h	
33	MAC	AES-CMAC		60h	
34	MAC	AES-CMAC (LSB)		3Dh	
35	CI Field	SITP command header long		C3h	Transport Layer (TPL)
36	Ident.Nr.	Meter-ID		78h	
37	Ident.Nr.	Meter-ID		56h	
38	Ident.Nr.	Meter-ID		34h	
39	Ident.Nr.	Meter-ID		12h	
40	Manufr	Meter-Manufacturer-ID		3Ah	
41	Manufr	Meter-Manufacturer-ID		63h	
42	Version	Meter-Version		55h	
43	Device type	Meter-Device-Type		20h	

44	Access No.	TPL Access Counter of GW		51h		
45	Status	GW State RSSI level (-66dBm)		20h		
46	Config Field	NNNNPIIIb		20h		
47	CRC 3			FBh	DLL	
48	CRC 3			1Bh		
49	Config Field	CCZMMMMMb		07h	TPL	
50	CFE	0VDDKKKKb		10h		
51	AES-Verify	Decryption verification	2Fh	28h		
52	AES-Verify	Decryption verification	2Fh	B2h		
53	SITP BL	Block length (28 bytes)	1Ch	73h	# 1	Application Layer (APL)
54	SITP BL	Block length	00h	59h		
55	SITP BID	Block ID field	00h	ACh		
56	SITP BCF	Block control filed	20h	9Bh		
57	SITP Rec. ID	Recipient ID: No dedicated application	00h	83h		
58	SITP DSI	DSI Auth. AES128-CMAC (8 Byte MAC)	32h	ABh		
59	SITP DSH1	Wrapper Key ID	20h	CDh		
60	SITP DSH2	Wrapper Key Version	00h	C8h		
61	SITP DS Key counter	Authentication Key counter = 15	0Fh	7Fh		
62	SITP DS Key counter	Authentication Key counter	00h	FDh		
63	SITP DS Key counter	Authentication Key counter	00h	F8h		
64	SITP DS Key counter	Authentication Key counter	00h	F2h		
65	CRC 4			BAh	DLL	
66	CRC 4			D9h		
67	SITP DS Target Time	Target time "zero" for immediate action	00h	FEh	# 1	Application Layer (APL)
68	SITP DS Target Time	Target time	00h	8Eh		
69	SITP DS Target Time	Target time	00h	1Eh	# 2	
70	SITP DS Target Time	Target time	00h	D8h		
71	SITP DS Target Time	Target time	30h	F1h		
72	SITP DS PID	Protocol ID: M-Bus	01h	97h		
73	SITP DS APDU	DIF (8 bit integer)	01h	18h		
74	SITP DS APDU	VIF (2nd Extension table)	FDh	B7h		
75	SITP DS APDU	VIFE (Remote control)	1Fh	43h		
76	SITP DS APDU	Value (breaker disconnect)	00h	4Ch		
77	SITP DS MAC	MAC	FAh	5Eh		
78	SITP DS MAC	MAC	41h	AEh		
79	SITP DS MAC	MAC	E2h	D8h		
80	SITP DS MAC	MAC	81h	66h		
81	SITP DS MAC	MAC	2Dh	3Fh		
82	SITP DS MAC	MAC	44h	15h		
83	CRC 5			F3h	DLL	
84	CRC 5			3Ah		
85	SITP DS MAC	MAC	9Bh	C5h	# 2	APL
86	SITP DS MAC	MAC	4Dh	CAh		
87	CRC 6			A1h	DLL	
88	CRC 6			38h		

N.11.3 RSP-UD (wM-Bus Set Breaker - successful)

Breaker example	
Medium	Breaker
Manufacturer	XYZ (633A)
Ident number	12345678
Version	85
Current state	connected (01h)

GW example	
Medium/device type	Communication Controller
Manufacturer	XYZ (633A)
Ident number	87654321
Version	8

ToDo:
1. Calculate Session Keys
2. Encrypt Message using Kenc
3. Calculate MAC using Kmac
4. Calculate CRCs

Individual Master Key Mk (see 9.1):
= 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

Message Counter CM RSP-UD (LSB first):
= F1 0A 00 00

'Encryption Session Key Kenc RSP-UD
= CMAC(Mk, 0x00 || MCR || IdentNo || padding) = CMAC(Mk,00||F1||0A||00||00||78||56||34||12 … ... ||07||07||07||07||07||07||07) = B1 F1 00 E8 F4 3B B4 48 02 95 F1 DC 4F 73 16 55

MAC Session Key Kmac RSP-UD
= CMAC(Mk, 0x01 || MCR || IdentNo || padding) = CMAC(Mk,01||F1||0A||00||00||78||56||34||12 … ... ||07||07||07||07||07||07||07) = 2A DD 03 97 29 C2 85 3E 78 16 C5 DE 1C 21 BC 69

RSP-UD (wM-Bus successful command)

Byte No	Field Name	Content	Breaker -> GW Bytes [hex] plain	Breaker -> GW Bytes [hex] AES coded	Layer
1	L Field	Length of data (67 bytes)		43h	Data Link Layer (DLL)
2	C Field	Response User Data		08h	
3	M Field	Manufacturer code		3Ah	
4	M Field	Manufacturer code		63h	
5	A Field	Ident No LSB (BCD)		78h	
6	A Field	Ident No (BCD)		56h	
7	A Field	Ident No (BCD) (= 12345678)		34h	
8	A Field	Ident No MSB (BCD)		12h	
9	A Field	Version (or Generation number)		55h	
10	A Field	Device type (Breaker)		20h	
11	CRC 1			F2h	
12	CRC 1			4Fh	
13	CI Field	Extended Link Layer (short)		8Ch	ELL
14	CC Field	Communication Control (bidir., RX on)		84h	
15	Access No.	Access Number of GW		23h	
16	CI Field	Authentication and Fragmentation layer		90h	Authentication and Fragmentation Layer (AFL)
17	AFLL	AFL Length (all AFL bytes after AFLL)		0Fh	
18	FCL	Fragmentation Control Field (LSB)		00h	
19	FCL	Fragmentation Control Field (MSB)		2Ch	
20	MCL	Message Control Field		25h	
21	MCR	Message Counter CM (LSB)		F1h	
22	MCR	Message Counter CM		0Ah	
23	MCR	Message Counter CM (e.g. = 2801)		00h	
24	MCR	Message Counter CM (MSB)		00h	
25	MAC	AES-CMAC (MSB)		1Ch	
26	MAC	AES-CMAC		56h	
27	MAC	AES-CMAC		6Dh	
28	MAC	AES-CMAC		47h	
29	CRC 2			D3h	DLL
30	CRC 2			EEh	
31	MAC	AES-CMAC		ABh	AFL
32	MAC	AES-CMAC		61h	
33	MAC	AES-CMAC		87h	
34	MAC	AES-CMAC (LSB)		54h	
35	CI Field	SITP response header short		C4h	Transport Layer TPL
36	Access No.	TPL Access Counter of GW		51h	
37	Status	Status		00h	
38	Config Field	NNNNPIIIb		20h	
39	Config Field	CCZMMMMMb		07h	
40	CFE	0VDDKKKKb		10h	
41	AES-Verify	Decryption verification	2Fh	2Dh	

42	AES-Verify	Decryption verification	2Fh	A5h		
43	SITP BL	Block length (28 bytes)	1Ch	7Dh	# 1	APL
44	SITP BL	Block length	00h	88h		
45	SITP BID	Block ID field	00h	41h		
46	SITP BCF	Block control filed	A0h	81h		
47	CRC 3			FFh	DLL	
48	CRC 3			44h		
49	SITP Rec. ID	Recipient ID: No dedicated application	00h	E5h	# 1	Application Layer (APL)
50	SITP DSI	DSI Auth. AES128-CMAC (8 Byte MAC)	32h	37h		
51	SITP DSH1	Wrapper Key ID	20h	6Ch		
52	SITP DSH2	Wrapper Key Version	00h	0Fh		
53	SITP DS Key counter	Authentication Key counter = 15	0Fh	7Ch		
54	SITP DS Key counter	Authentication Key counter	00h	9Fh		
55	SITP DS Key counter	Authentication Key counter	00h	86h		
56	SITP DS Key counter	Authentication Key counter	00h	10h		
57	SITP DS Target Time	Target time "zero" for immediate action	00h	08h		
58	SITP DS Target Time	Target time	00h	22h		
59	SITP DS Target Time	Target time	00h	C3h	#2	
60	SITP DS Target Time	Target time	00h	3Ch		
61	SITP DS Target Time	Target time	30h	F7h		
62	SITP DS PID	Protocol ID: M-Bus	01h	CDh		
63	SITP DS APDU	DIF (8 bit integer)	01h	FDh		
64	SITP DS APDU	VIF (2nd Extension table)	FDh	B8h		
65	CRC 4			33h	DLL	
66	CRC 4			73h		
67	SITP DS APDU	VIFE (Remote control)	1Fh	41h	#2	Application Layer (APL)
68	SITP DS APDU	Value (breaker disconnected)	00h	1Ch		
69	SITP DS MAC	MAC	FAh	20h		
70	SITP DS MAC	MAC	41h	D4h		
71	SITP DS MAC	MAC	E2h	77h		
72	SITP DS MAC	MAC	81h	D8h		
73	SITP DS MAC	MAC	2Dh	C5h		
74	SITP DS MAC	MAC	44h	A6h		
75	SITP DS MAC	MAC	9Bh	7Fh		
76	SITP DS MAC	MAC	4Dh	37h		
77	CRC 5			57h	DLL	
78	CRC 5			29h		

N.11.4 RSP-UD (wM-Bus Set Breaker - failure)

Breaker example	
Medium	Breaker
Manufacturer	XYZ (633A)
Ident number	12345678
Version	85
Current state	connected (01h)

GW example	
Medium/device type	Communication Controller
Manufacturer	XYZ (633A)
Ident number	87654321
Version	8

ToDo:
1. Calculate Session Keys
2. Encrypt Message using Kenc
3. Calculate MAC using Kmac
4. Calculate CRCs

Individual Master Key Mk (see 9.1):
= 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

Message Counter CM RSP-UD (LSB first):
= F1 0A 00 00

'Encryption Session Key Kenc RSP-UD
= CMAC(Mk, 0x00 || MCR || IdentNo || padding) = CMAC(Mk,00||F1||0A||00||00||78||56||34||12 … ... ||07||07||07||07||07||07||07) = B1 F1 00 E8 F4 3B B4 48 02 95 F1 DC 4F 73 16 55

MAC Session Key Kmac RSP-UD
= CMAC(Mk, 0x01 || MCR || IdentNo || padding) = CMAC(Mk,01||F1||0A||00||00||78||56||34||12 … ... ||07||07||07||07||07||07||07) = 2A DD 03 97 29 C2 85 3E 78 16 C5 DE 1C 21 BC 69

RSP-UD (wM-Bus Key version error)

Byte No		OMS wM-Bus frame	Breaker -> GW		Layer
	Field Name	Content	Bytes [hex]		
			plain	AES coded	
1	L Field	Length of data (51 bytes)		33h	Data Link Layer (DLL)
2	C Field	Response User Data		08h	
3	M Field	Manufacturer code		3Ah	
4	M Field	Manufacturer code		63h	
5	A Field	Ident No LSB (BCD)		78h	
6	A Field	Ident No (BCD)		56h	
7	A Field	Ident No (BCD) (= 12345678)		34h	
8	A Field	Ident No MSB (BCD)		12h	
9	A Field	Version (or Generation number)		55h	
10	A Field	Device type (Breaker)		20h	
11	CRC 1			71h	
12	CRC 1			58h	
13	CI Field	Extended Link Layer (short)		8Ch	ELL
14	CC Field	Communication Control (bidi., RX on)		84h	
15	Access No.	Access Number of GW		23h	
16	CI Field	Authentication and Fragmentation layer		90h	Authentication and Fragmentation Layer (AFL)
17	AFLL	AFL Length (all AFL bytes after AFLL)		0Fh	
18	FCL	Fragmentation Control Field (LSB)		00h	
19	FCL	Fragmentation Control Field (MSB)		2Ch	
20	MCL	Message Control Field		25h	
21	MCR	Message Counter C_M (LSB)		F1h	
22	MCR	Message Counter C_M		0Ah	
23	MCR	Message Counter C_M (e.g. = 2801)		00h	
24	MCR	Message Counter C_M (MSB)		00h	
25	MAC	AES-CMAC (MSB)		42h	
26	MAC	AES-CMAC		2Fh	
27	MAC	AES-CMAC		B1h	
28	MAC	AES-CMAC		26h	
29	CRC 2			DEh	DLL
30	CRC 2			C8h	
31	MAC	AES-CMAC		14h	AFL
32	MAC	AES-CMAC		37h	
33	MAC	AES-CMAC		55h	
34	MAC	AES-CMAC (LSB)		97h	
35	CI Field	SITP response header short		C4h	Transport Layer TPL
36	Access No.	TPL Access Counter of GW		51h	
37	Status	Status (application error)		02h	
38	Config Field	NNNNPIIIb (TPL-Padding)		18h	
39	Config Field	CCZMMMMMb		07h	
40	CFE	0VDDKKKKb		10h	
41	AES-Verify	Decryption verification	2Fh	B3h	

42	AES-Verify	Decryption verification	2Fh	15h		
43	SITP BL	Block length (7 bytes)	07h	C2h	# 1	APL
44	SITP BL	Block length	00h	E1h		
45	SITP BID	Block ID field	00h	A0h		
46	SITP BCF	Block control filed	A0h	72h		
47	CRC 3			39h	DLL	
48	CRC 3			2Eh		
49	SITP Rec. ID	Recipient ID: No dedicated application	00h	1Eh	# 1	APL
50	SITP DSI	DSI Status response	22h	E7h		
51	SITP DSH1	Key ID	20h	4Eh		
52	SITP DSH2	Key Version	00h	35h		
53	SITP SR	Stat. Rsp. "DSH error: Unknown or invalid Key ID/Version"	19h	03h		
54	TPL-Padding	Padding	05h	ADh	#1	TPL
55	TPL-Padding	Padding	05h	47h		
56	TPL-Padding	Padding	05h	9Fh		
57	TPL-Padding	Padding	05h	0Fh		
58	TPL-Padding	Padding	05h	0Dh		
59	CRC 4			12h	DLL	
60	CRC 4			41h		