



Open Metering System Specification

Requirements for OMS use case support

**Annex M to
Volume 2 Primary Communication
Issue 4.5.1**

RELEASE B (2022-12)

Document History

Version	Date	Comment	Editor
A 0.0.1	2017-03-22	Setup of table for Clock Sync for initial discussion	Hartmut Ritter, Joachim Baumann
A 0.0.2	2017-03-26	Modified UC-04 table according to input from Uwe Pahl, copied short use case description from document "Open Metering Spec. Use Cases" Issue 1.0.2	Hartmut Ritter
A 0.0.3	2017-03-27	Removed references, minor edits	Joachim Baumann
A 0.0.4	2017-10-16	Add result from Action #66-16, #67-12, -14, -18	Uwe Pahl
A 0.0.5	2017-12-11	Add result from Action #67-9, #67-14, Add new UC-05 by Action #68-8 Add new UC-08 by Action #68-12 Add new UC-09 by Action #68-13	Uwe Pahl
A 0.0.6	2018-01-16	Updated UC-05 according to actions #69-1 and #69-12	Alexander Rohleder
A 0.0.7	2018-02-05	Consolidated version with all changes until 2018-02-03	Achim Reissinger
A 0.0.8	2018-02-20	Comments for A 0.0.7 added	Dirk Matussek, Ronald Müller, Joachim Baumann, Achim Reissinger
A 0.0.9	2018-03-14, 2018-03-15 and 2018-03-19	Changes in M.1.5 and M.2.2 to M.2.4, TOC added, Chapter M.1.6 added, Adaptation of all UCs to table M.3	AG1, Achim Reissinger
A 0.0.10	2018-04-26 and 2018-05-02	Changes in UC-05, UC-06 and UC-08, Introduction of Seq_SND-UDx in all use cases	AG1, Achim Reissinger
A 0.0.11	2018-06-20	Changes in UC-03, UC-04 and UC-05	AG1, Achim Reissinger
A 0.0.12	2018-10-04	Consolidated version of three documents	AG1, Achim Reissinger
A 0.0.13	2018-10-16	Corrections for Seq_SND-UDx, Seq_SND-UD2	Dirk Matussek, Achim Reissinger
A 0.0.14	2018-11-12	Introduction of new abbreviations Consolidation of M.1.2, M.2.5 and M.2.7	Ronald Müller, Thomas Blank, Achim Reissinger
A 0.0.15	2019-01-25	Consolidation of UC-04, UC-07 and UC-09 and further changes by Action #82-15	Achim Reissinger
A 0.0.16	2019-02-19	Consolidation	Achim Reissinger, Thomas Blank, Dirk Matussek
A 0.0.17	2019-04-03	Correction of abbreviation KeyID and KeyVersion, removal of Seq_REQ-UD2 [MBus-Data] in tables M.5, M.19 and M.21, change of headlines for tables M.8 to M.11	Achim Reissinger
A 0.0.18	2019-04-26	UC-02: deletion of all content, marking as reserved UC-04: Correction of headlines in tables M.7 to M.10	Achim Reissinger, Thomas Blank
A 0.0.19	2019-07-03	Consolidation of UC-04, UC-06, UC-07, UC-08 and UC-09 Adjustment of table numbers to OMS-S2	Achim Reissinger
A 0.0.20	2019-09-20	Consolidation of whole document	Achim Reissinger
A 0.0.21	2019-10-19	Processing of editorial comments	Achim Reissinger
A 0.0.22	2019-10-27	UC-07 updated	AG1, Achim Reissinger
A 0.0.23	2019-11-04	Processing of editorial comments	Achim Reissinger
A 0.0.24	2019-11-14	Processing of all comments	AG1, Achim Reissinger
A 0.0.25	2020-01-29 2020-02-02	Review of whole document Splitting of the entry "Data elements" in the UC-01, UC-03, UC-04, UC-06 and UC-07	AG1 Achim Reissinger
A 0.0.26	2020-02-18	Changes in "Data elements" boxes during	AG1

Version	Date	Comment	Editor
		meeting #98	
A 0.0.27	2020-03-11	Adoption of all changes from A 0.0.26 Editorial corrections Implementation of action item proposals: addition of BCF values in several UCs, changes for UC-04	Achim Reissinger
A 0.0.28	2020-03-18	Review of whole document, editorial corrections	AG1, Achim Reissinger
A 0.0.29	2020-03-24	Replacement of "meter" and "meters" with "meter/actuator" and "meters/actuators" Addition of reference to Annex P in chapter M.1.4	Achim Reissinger
A 0.0.30	2020-03-26	Revision based on comments by Thomas Banz	Thomas Banz, Achim Reissinger
A 0.0.31	2020-04-03	Revision based on sub group meetings and additional input Addition of chapter M.1.5	AG1, Achim Reissinger
A 0.1.0	2020-04-22	Add footnote c in Table M.22 + M.23 Draft version for review by AG3	Achim Reissinger, Uwe Pahl
A 0.1.1	2020-05-26 and 2020-05-29	Editing during meeting #100 Update of table numbers because of changed table numbering in OMS-S2 V 4.3.x	AG1, Achim Reissinger Achim Reissinger
A 0.1.2	2020-05-30	Update Tab.23 (remove footnote b, c, d; move footnote a to b; add new footnote a, remove col. "Obligation", add col. "freq. trans."; add dev.type 21h) Update Appendix A acc. to AG1+AG3 Joint#03	Uwe Pahl
A 0.1.3	2020-06-02	Fixed remaining footnote c in Tab. M.23	Achim Reissinger
A 0.1.4	2020-06-09	Update M.1.1 and add M2.2 OMS-UC-00	Uwe Pahl
A 0.2.0	2020-06-15 and 2020-06-17	Editing during meeting #101 Addition of agreed editorial changes from joint meeting #3 with AG3	AG1, Achim Reissinger Achim Reissinger
A 0.2.1	2020-07-07	Integration of comments from AG1 internal review: M.1.1 changed M.1.2 changed M.2.2 wording changed Tab. M.1 changed Tab. M.24 changed Tab. M.20: note added (after table) Tab. M.26 changed	Achim Reissinger
A 1.0.0	2020-09-24 and 2020-09-29 and 2020-09-30 and 2020-10-02	Editorial changes Tab. M.14 and M.15: Extension for footnote a M.1.5 changed M.2.7 changed: UC-05, Activation Command and Termination Command M.2.6 changed Editorial changes	Achim Reissinger Thomas Blank, Uwe Pahl Thomas Blank, Uwe Pahl Achim Reissinger
A 1.0.1	2020-10-09	M.2.6 UC-04 changed	Thomas Blank, Uwe Pahl

Version	Date	Comment	Editor
	And 2020-10-13	and M.1.7 changed (CNF-IR optional) M.2.9 changed to reserved	Thomas Banz, Achim Reissinger
A 1.0.2	2020-10-16	M.2.9 changed	Achim Reissinger
A 1.0.3	2020-10-22 and 2022-05-30	Editorial changes Copyright remark added to front page Release	Achim Reissinger
B 1.0.5	2022-01-18 and 2022-01-31 and 2022-08-02 and 2022-08-09 and 2022-09-14 and 2022-10-04 and 2022-10-09 and 2022-10-15	M.2.9 revised M.1.5 reference corrected UC-07, UC-10, UC-12, UC-14, UC-20 added Introduction of term "OMS end-device" Table M.6 changed "OMS end-device" includes "actuator" M.1.5 changed Editorial changes (referenced table numbers) DSI=32h in all tables deleted Sub-headlines reformatted Tables M.38 and M .39 changed UC-10 and UC-20 removed Term "application key" replaced by "application security key" Term "key material" replaced by "keying material" Release Candidate	AG1 Achim Reissinger Joachim Baumann
B 1.0.6	2022-11-05	Integration of review comments Release	AG1, Achim Reissinger

Contents

Document History	2
Contents	5
Tables	6
Figures	7
M.1 General	8
M.1.1 Scope	8
M.1.2 Description of a General Understanding of Roles for Use Cases	8
M.1.3 Unidirectional Modes (Wireless M-Bus)	8
M.1.4 Bidirectional Modes	8
M.1.5 Commands and Command Responses	9
M.1.6 Data Points	9
M.1.7 Basic Communication Sequences	9
M.1.8 Application Protocols	14
M.2 Functional Requirements per Individual Use-Case	15
M.2.1 Description	15
M.2.2 OMS-UC-00 Conformance Test (mandatory)	15
M.2.3 OMS-UC-01 OMS End-device Registration	18
M.2.4 OMS-UC-03 Disconnection & Reconnection	19
M.2.5 OMS-UC-04 Clock Management	22
M.2.6 OMS-UC-05 Firmware Update	27
M.2.7 OMS-UC-06 OMS End-device Supervision	34
M.2.8 OMS-UC-07 Consumer Information	36
M.2.9 OMS-UC-08 Key Management	41
M.2.10 OMS-UC-12 Application Management	45
M.2.10.1 Overview	45
M.2.10.2 OMS-UC-12a Due Date Management	45
M.2.10.3 OMS-UC-12b Customer Ownership Number	48
M.2.11 OMS-UC-14 Data Selection	49
Appendix M.A (informative)	51
Example for the Renewal of the Master Key OMS-UC-08	51

Tables

Table M.1 – Basic Link Layer communication sequences.....	10
Table M.2 – Application protocols.....	14
Table M.3 – OMS-CT Value RC2	15
Table M.4 – OMS conformance test command.....	16
Table M.5 – Requirements for OMS-UC-00; OMS CT command.....	17
Table M.6 – Example sequences of OMS conformance test command/response.....	17
Table M.7 – Requirements for OMS-UC-01; requirements for OMS end-device Registration	18
Table M.8 – State definitions	19
Table M.9 – Requirements for OMS-UC-03; get state information	20
Table M.10 – Requirements for OMS-UC-03; set control state	21
Table M.11 – Requirements for OMS-UC-04; Allowed combinations of functions.....	23
Table M.12 – Requirements for function "Read Time"	23
Table M.13 – Requirements for function "Adjust Clock Time by Gateway"	24
Table M.14 – Requirements for function "Adjust Clock Time by Head-End"	25
Table M.15 – Requirements for function "Set Date and Time by Head-End"	26
Table M.16 – Requirements for OMS-UC-05; State Command & Response	27
Table M.17 – Requirements for OMS-UC-05; Prepare Command & Response	28
Table M.18 – Requirements for OMS-UC-05; Transfer Command	29
Table M.19 – Requirements for OMS-UC-05; Completion Command & Response.....	30
Table M.20 – Requirements for OMS-UC-05; Validate Command & Response.....	31
Table M.21 – Requirements for OMS-UC-05; Activate Command & Response	32
Table M.22 – Requirements for OMS-UC-05; Terminate Command & Response.....	33
Table M.23 – Requirements for OMS-UC-06; get status information	34
Table M.24 – Requirements for OMS-UC-06; clear status information	35
Table M.25 – Sub use cases for OMS-UC-07.....	36
Table M.26 – Requirements for OMS-UC-07, get consumer information	39
Table M.27 – Requirements for OMS-UC-07, mandatory data elements	40
Table M.28 – Requirements for OMS-UC-08; Get list of keys.....	42
Table M.29 – Requirements for OMS-UC-08; Transfer of keying material	43
Table M.30 – Requirements for OMS-UC-08; Activation/Deactivation of keying material.....	44
Table M.31 – Harmonised configuration functions	45
Table M.32 – Requirements for OMS-UC-12a; Get last due date	45
Table M.33 – Requirements for OMS-UC-12a; Get next due date.....	46
Table M.34 – Requirements for OMS-UC-12a; Set next due date	47

Table M.35 – Requirements for OMS-UC-12b; Get ownership number	48
Table M.36 – Requirements for OMS-UC-12b; Set ownership number.....	48
Table M.37 – Requirements for OMS-UC-14; Data point selection	49
Table M.38 – Example for data point selection in Application 7, block 0	50

Figures

Figure 1 – Disconnecter overview	19
Figure 2 – Scenarios for the data transfer to the display via gateway or AMM-HES	37
Figure 3 – Scenario for the direct data transfer to the display	38

M.1 General

M.1.1 Scope

The [OMS-S2] defines requirements to be fulfilled by OMS end-devices. Beside these requirements, the OMS end-device may also support additional use cases described in this annex.

If the manufacturer declares the support of a use case in the [ManDec], then the OMS end-device shall fulfil all respective requirements in this annex in order to pass the tests in the [OMS-CT]. Additionally, if at least one bidirectional use case (see M.2.2) is declared, the use case OMS-UC-00 shall also be supported.

M.1.2 Description of a General Understanding of Roles for Use Cases

The general roles of the market players according to the European legislation for the internal energy markets are described in [OMS-S1], 3.1 and [OMS-S1], Annex A.

To process a use case, the role-owner requires appropriate system related rights and the required metering point related information such as Ident. No. and related communication and application access rights.

It is not in the scope of this document to allocate any use cases to any market roles. It is the responsibility of the market players to execute the roles as needed and to distribute the correlated communication and application security keys accordingly.

The use cases and their related security requirements described in this document will provide a tool-set of functions for the different market players to fulfil their roles.

Each use case defines security requirements for the OMS end-device and a set of KeyIDs as defined in [OMS-S2], 9.2.2. Security profiles are defined in [OMS-S2], 9.1. The OMS end-device shall fulfil these requirements in order to serve and react according to the use case. However, it is not up to the individual OMS end-device to allocate and distribute the various rights to each user.

M.1.3 Unidirectional Modes (Wireless M-Bus)

Unidirectional operation modes are only supported by wireless OMS end-devices. In this mode the OMS end-device frequently transmits datagrams containing OMS end-device identification together with OMS end-device data.

M.1.4 Bidirectional Modes

Bidirectional OMS end-devices provide the possibility of a gateway to OMS end-device communication.

For wireless OMS end-devices the EN 13757-4 defines rules how to access such OMS end-devices (EN 13757-4:2019 subclause 12.6.3).

The accessibility of wired OMS end-devices is defined in Annex P.

A bidirectional wireless OMS end-device additionally applies unidirectional communication sequences like SND-NR. Parts of a use case or a complete use case can be fulfilled by unidirectional sequences.

The minimum requirement for an OMS end-device to support bidirectional use cases is to process one command per message unless otherwise defined in the specific use case. Sending several commands per message is not recommended and may lead to an unexpected behaviour of the OMS end-device.

M.1.5 Commands and Command Responses

This chapter provides general information on command handling related topics. It explains communication rules and the possibility to recognise successful or not successful commands.

The communication partner e.g. the gateway may send commands to the OMS end-device. After the command execution, the communication partner may request the command response. The communication partner shall identify a corresponding command response by the ALA and a matching TPL access number of the OMS end-device message (RSP-UD) with the TPL access number of the corresponding request (SND-UD2 or REQ-UD2, see [OMS-S2], 7.2.2).

The command execution inside an OMS end-device shall be processed at latest within 120 seconds (unless otherwise defined in the specific use case). The processing time starts with the reception of the command or (in case) after a delay or absolute start time that is indicated by the TargetTime in an SITP command (see [EN13757-7:2018], clause A.9.1).

A successful command results in a command response (acc. to [OMS-S2], 8.2.5, Figure 15). A command response shall either be a dedicated response providing the specified MB-Data-Tags or an unspecific response if there are “no requirements” in the data elements from the OMS end-device. An unspecific response shall be either:

- the standard response,
- a response with other M-Bus tags or
- an empty response.

An empty response shall provide at least one idle filler byte in the application layer (e.g. 2Fh for the M-Bus protocol).

NOTE: The idle filler ensures at least one encrypted block in case of encryption. If no encryption is applied, the idle filler ensures that the application layer is not empty.

A not successful command results in an error response (acc. to [OMS-S2], 8.2.5, Figure 15). An error response contains an error according to [OMS-S2], 8.8, Table 37.

The successful or erroneous execution of the command is also indicated by the status byte of the corresponding ACK/RSP-UD (see [OMS-S2], 7.2.3). As long as the application does not finish the processing of the command the Transport layer shall respond with the command state “application busy”.

Note that the indication of the command state in the status byte is a new feature supported from OMS-Spec. Volume 2 V4.2.1. Devices conforming to an older version of the OMS-specification may respond a “no error” even if the command execution fails. For such devices, the RSP-UD should always be requested.

Annex N provides example datagrams of commands and command responses.

M.1.6 Data Points

The MB-Tags (MB-Data-Tag for data points, MB-Command-Tag for commands) used in this document to describe data points are defined in Annex B.

M.1.7 Basic Communication Sequences

Table M.1 lists the basic uni- and bidirectional Link Layer communication sequences used to implement the OMS use cases. The Link Layer message types used in the sequences between the gateway and the OMS end-device are described as well as the respective error treatment on both sides.

For timing details see EN 13757-4:2019 Annex E. The dependencies of message types are shown in [OMS-S2], Table 12 and Table 13.

Table M.1 – Basic Link Layer communication sequences

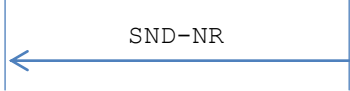
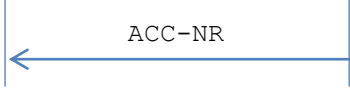
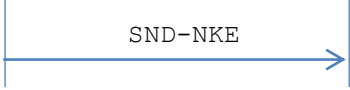
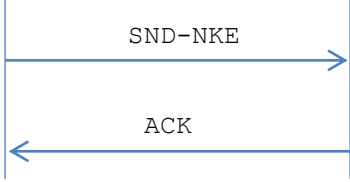
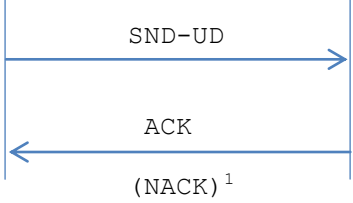
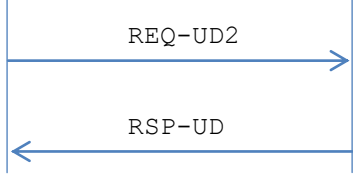
Sequence name	Description	Wireless unidir.	Wireless bidir.	Wired
Seq_SND-NR	<p>  </p> <p>Description: Transmits standard data in wireless communication. Informs about the accessibility of a wireless OMS end-device.</p>	X	X	
Seq_ACC-NR	<p>  </p> <p>Description: Informs about the accessibility of a wireless OMS end-device. May be used by unidirectional wireless OMS end-devices to maintain the synchronous transmission timing without sending metering data.</p>	X	X	
Seq_SND-NKE	<p>Wireless bidirectional:</p> <p>  </p> <p>Description: Resets the link and ends the FAC. Each communication session shall be terminated by the gateway sending a SND-NKE. In this document, Seq_SND-NKE is not mentioned explicitly in the description of the use-cases.</p> <p>Wired:</p> <p>  </p> <p>Description: Pre-sets the internal last received FCB-bit and clears the optional selection bit.</p>		X	X

Table M.1 – Basic Link Layer communication sequences (cont.)

Sequence name	Description	Wireless unidir.	Wireless bidir.	Wired
Seq_SND-UD	<p><u>Gateway</u> <u>OMS end-device</u></p>  <p><u>Description:</u> The gateway sends data or a command to the OMS end-device. The OMS end-device acknowledges the reception of the data or the command (link layer acknowledgement).</p> <p><u>Error treatment gateway (wireless only):</u> As long as the gateway does not receive an ACK or NACK response, it tries to repeat the SND-UD as specified in [OMS-S2], Annex I.</p> <p><u>Error treatment wireless OMS end-device:</u> The OMS end-device responds with a NACK as specified in [OMS-S2], 5.2.3.</p>		X	X
Seq_REQ-UD2	<p><u>Gateway</u> <u>OMS end-device</u></p>  <p><u>Description:</u> The gateway requests the OMS end-device's application data. The OMS end-device responds with its application data.</p> <p><u>Error treatment gateway (wireless only):</u> As long as the gateway does not receive an RSP-UD, it tries to repeat the REQ-UD2 (number of repetitions according to Annex I).</p>		X	X

¹ The NACK message is supported by wireless bidirectional OMS end-devices only.

Table M.1 – Basic Link Layer communication sequences (cont.)

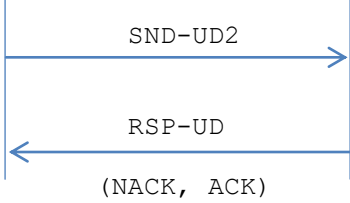
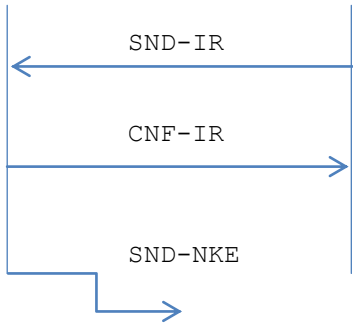
Sequence name	Description	Wireless unidir.	Wireless bidir.	Wired
Seq_SND-UD2	<p><u>Gateway</u> <u>OMS end-device</u></p>  <p><u>Description:</u> The gateway sends data or a command to the OMS end-device. The OMS end-device responds with its application data. This sequence may replace the combination of a SND-UD – ACK and a subsequent REQ-UD2 – RSP-UD sequence. An OMS end-device implementing this sequence shall also support the combination of a SND-UD – ACK and a subsequent REQ-UD2 – RSP-UD sequence.</p> <p><u>Error treatment gateway (wireless only):</u> As long as the gateway does not receive a RSP-UD or NACK response, it tries to repeat the SND-UD2. If the OMS end-device responds with ACK, the gateway shall assume that the OMS end-device does not support SND-UD2 and thus retry with SND-UD.</p> <p><u>Error treatment OMS end-device (wireless only):</u> The OMS end-device responds with a NACK as specified in [OMS-S2], 5.2.3.</p>		X	X
Seq_SND-UDx	<p>This sequence can be implemented</p> <ul style="list-style-type: none"> • either by the combination of a Seq_SND-UD and a subsequent Seq_REQ-UD2 • or by the Seq_SND-UD2 		X	X

Table M.1 – Basic Link Layer communication sequences (cont.)

Sequence name	Description	Wireless unidir.	Wireless bidir.	Wired
Seq_SND-IR	<p>  <pre> sequenceDiagram participant Gateway participant OMS_end_device as OMS end-device OMS_end_device->>Gateway: SND-IR Gateway-->>OMS_end_device: CNF-IR Gateway->>OMS_end_device: SND-NKE </pre> <p><u>Description:</u> The OMS end-device sends an installation request to the gateway. The gateway may confirm with a CNF-IR in case it accepts the OMS end-device's installation request, see [OMS-S2], 5.2.5. The SND-NKE may be received by an installation tool.</p> </p>	X	X	

M.1.8 Application Protocols

The message types SND-UD, SND-UD2 or RSP-UD are used in different use cases and in different application protocols. The following table introduces the name of the application protocol and its meaning according to the definitions of [OMS-S2], Table 1.

Table M.2 – Application protocols

Name of Application protocol	Explanation (refer to [OMS-S2] Table 1)	CI-Field for Wireless M-Bus	CI-Field for Wired M-Bus
App-Select	Command “Application Reset or Select” followed by some subfield to select a special application	53h	50h
App-Reset	Command “Application Reset or Select” without some subfield used to reset application to standard response	53h	50h
App-Error	Response “Application Error” signalling an error in command execution	6Eh, 6Fh	70h
Dev-Select	“Selection of Device” used for secondary addressing	-	52h
MBus-Cmd	Command of M-Bus protocol	5Bh	51h, 5Ah
MBus-Data	Response of M-Bus protocol	7Ah, 72h	72h
Clock-Sync	Command of Clock Synchronisation protocol	6Ch, 6Dh	6Ch, 6Dh
ITP-Cmd	Command of Image Transfer protocol	C0h	C0h
ITP-Rsp	Response of Image Transfer protocol	C1h, C2h	C2h
SITP-Cmd	Command of Security Information Transport protocol	C3h	C3h
SITP-Rsp	Response of Security Information Transport protocol	C4h, C5h	C5h

M.2 Functional Requirements per Individual Use-Case

M.2.1 Description

The tables in the following chapters list the functional requirements (like data items and protocols) for the respective use-case.

M.2.2 OMS-UC-00 Conformance Test (mandatory)

OMS-UC-00 is designed to check the bidirectional functionality of an OMS end-device according to [OMS-S2], 8.2.5 during the OMS conformance test. Therefore, this use case becomes mandatory if at least one other bidirectional use case is implemented. These are all use case of this annex except the use case:

- UC-01 and
- UC-07 (in case data are provided only by unidirectional communication sequences).

The OMS Conformance Test command is an extension of the standardised remote control command according to [EN13757-3:2018], Annex E.2.

The first parameter byte RC1 has during conformance test a fix value to disable all radio specific tests (see [EN13757-3:2018] Tables E.8 to E10).

The second parameter byte RC2 shall be according to Table M.3.

Table M.3 – OMS-CT Value RC2

b7	b6	b5	b4	b3	b2	b1	b0
0 ^a	0 ^a	1 ^a	1 ^a	Function of OMS-CT command (see "Value RC2" in Table M.4)			
^a reserved for future use							

The OMS conformance test command allows following test functions:

Table M.4 – OMS conformance test command

Name	MB-Command tag acc. to Annex B	Set of values			Response of test device	Access rights
		Value RC1	Value RC2	Test function		
OMC-CT command	XCT1!	40h/ C0h ^a	30h	Application error	The parameter value 30h shall intentionally not be supported. The OMS end-device shall react with an application error 15h acc. to [OMS-S2], 8.8.	R
		40h/ C0h ^a	31h	Empty or standard response	The device responds the typical unspecific response acc. to M.1.5.	R
		40h/ C0h ^a	32h	Test response short	The device responds this MB-Tag with a fix 2 byte pattern '42h 42h'	R
		40h/ C0h ^a	33h	Test response long	The device responds this MB-Tag with a pattern N times '43h', where N must be selected in a manner that the response corresponds to the maximum supported datagram length that can be transmitted.	R
		40h/ C0h ^a	34h	Test command long	The sender transmits test pattern ^b in a datagram with max. package size acc. to [OMS-S2], 5.2.2 The receiver shall respond with the last 4 bytes of the test pattern sequence.	R
		40h/ C0h ^a	35h.. 3Fh	Reserved for future use		-
^a Bit7 in RC1 is currently marked as reserved in EN13757-3:2018. The OMS end-device shall support the OMS-CT command independent of this bit state and responds the same RC1 value. ^b The applied test pattern in the command shall be in the range 20h to 7Eh. (Type LVAR according to EN13757-3:2018, Table 5).						

The OMS conformance test command shall be applied according to Table M.5.

Table M.5 – Requirements for OMS-UC-00; OMS CT command

Functional	Wireless	Wired
Communication sequences unidirectional	N/A	N/A
Communication sequences bidirectional	Seq_SND-UDx [MBus-Cmd]	Seq_SND-UDx [MBus-Cmd]
Data elements to the OMS end-device	MB.Command-Tag: <ul style="list-style-type: none">• XCT1!	
Data elements from the OMS end-device	MB-Data-Tag: <ul style="list-style-type: none">• CT1!, the value depends on command function (see Table M.4).	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41, Encryption and Authentication according to [OMS-S2], Table 39 Optionally, the device may apply Application security with: <ul style="list-style-type: none">• ASP10 according to [OMS-S2], Table 44• BCF=20h/A0h acc. to [EN13757-7:2018], Table A.3• PID=01h acc. to [EN13757-7:2018], Table A.14• KeyID=1Fh• TargetTime set to "zero" (3000000000h) for immediate action	
NOTE: If the device supports ASP10, it may refuse the execution of the OMS-CT command without application security to protect against misuse of the OMS conformance test command.		

The lifetime of the OMS CT response shall be like any other command response acc. to [OMS-S2], 8.2.5.

Table M.6 provide examples of the M-Bus records in the command and related response message with OMS conformance test commands.

Table M.6 – Example sequences of OMS conformance test command/response

Test function	Command (hex)	Response (hex)
Test response short	02 FD 9F 1D 40 32	04 FD 9F 1D 40 32 42 42
Test response long	02 FD 9F 1D C0 33	0D FD 9F 1D A2 C0 33 43 ... 43 (A0 times 43)
Test command long	0D FD 9F 1D 50 40 34 6E 6D 6C ... 25 24 23 22 21	06 FD 9F 1D 40 34 24 23 22 21

M.2.3 OMS-UC-01 OMS End-device Registration

OMS end-device registration is the process of detecting new OMS end-devices and registering an OMS end-device to a master (see [OMS-S2], 8.2.2).

If a wireless OMS end-device receives a valid CNF-IR it may stop the transmission of SND-IR even if less than 6 times SND-IR has been sent.

Table M.7 – Requirements for OMS-UC-01; requirements for OMS end-device Registration

Functional	Wireless	Wired
Communication sequences unidirectional	Seq_SND-IR (manually initiated)	N/A
Communication sequences bidirectional	Seq_SND-IR (manually initiated)	Primary addresses: Seq_REQ-UD2 [MBus-Data] or Secondary address: Seq_SND-UDx [Dev-Select, MBus-Data] or Wildcard searching procedure: Seq_SND-UDx [Dev-Select, MBus-Data]
Data elements to the OMS end-device	N/A	MB-Data-Tag: <ul style="list-style-type: none"> ID1! (optional)
Data elements from the OMS end-device	No requirements	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41, Encryption and Authentication according to [OMS-S2], Table 39	

M.2.4 OMS-UC-03 Disconnection & Reconnection

This use case describes how a gateway obtains or sets control state of a disconnector (breaker or valve).

Devices such as breakers or valves can switch the flow of a medium. Such devices (disconnectors) share their current physical status with DC2! (output state) and their internal status of the control object with DC1! (control state). The master shall use XDC1! as content of a SND-UD to change the control state.

Two different types of disconnectors are available.

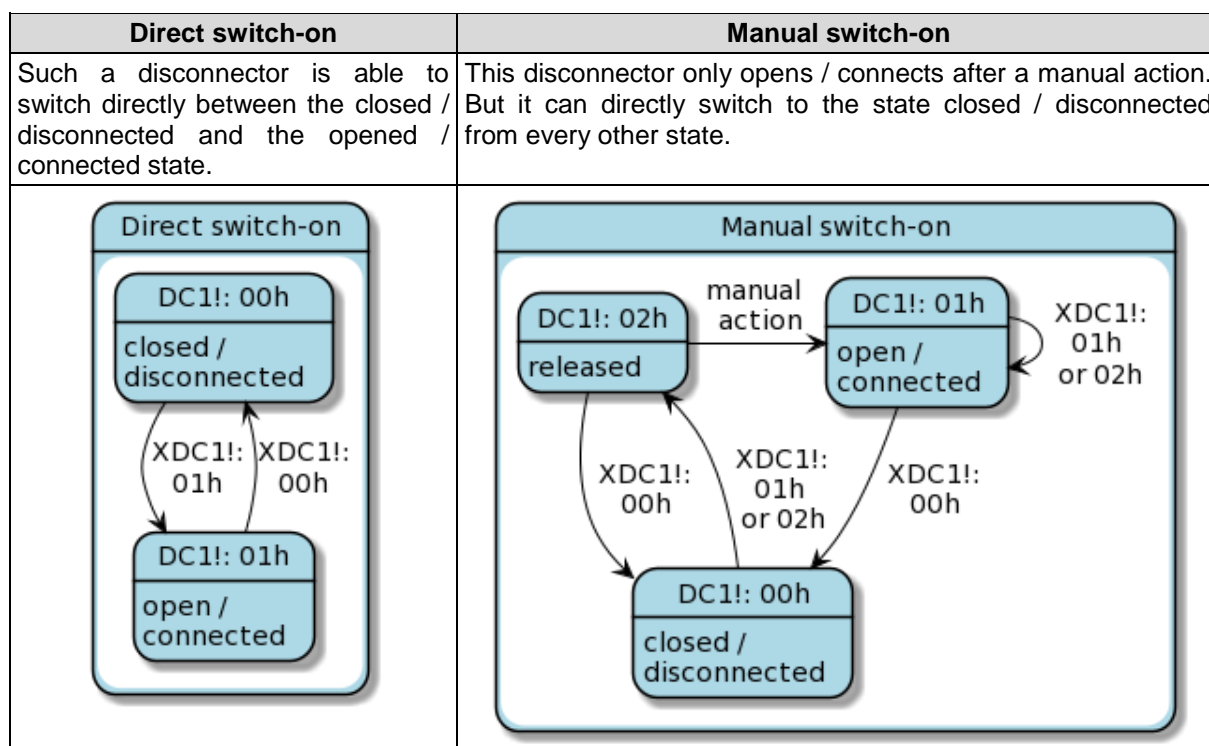


Figure 1 – Disconnector overview

Figure 1 shows the control states of the disconnector only.

For a disconnector, as the typical actuator, the maximum time interval between transmissions shall be the same as the maximum update interval for meter transmissions of the same medium (i.e. electricity or others) as shown in [OMS-S2], 4.3.2.2.

The disconnector states shall be applied according to the following definitions:

Table M.8 – State definitions

Name	MB- Tag acc. to Annex B	Set of values			Access rights
		Value	Valve	Breaker	
Internal state of the disconnector control object	DC1!	00b	closed	disconnected	R
		01b	opened	connected	R
		10b ^a	released	released	R
Output state of the disconnector	DC2!	00b	closed	disconnected	R
		01b	opened	connected	R
Set control state of disconnector	XDC1!	00b	close	disconnect	W
		01b	open	connect	W
		10b ^a	release	release	W

^a Service is only available for type “Manual switch-on”.

If the disconnecter functionality is a function of a meter (using the device type of a meter), subunit 1 shall be used in data information block (according to [EN 13757-3:2018], Annex C.3).

Table M.9 delivers the current states of the breaker / valve according to [EN13757-3:2018], Annex C.3

Table M.9 – Requirements for OMS-UC-03; get state information

Functional	Wireless	Wired
Communication sequences unidirectional	Seq_SND-NR	N/A
Communication sequences bidirectional	Seq_SND-UDx [App-Reset, MBus-Data]	Seq_SND-UDx [App-Reset, MBus-Data]
Data elements to the OMS end-device	No requirements	
Data elements from the OMS end-device	MB-Data-Tag: <ul style="list-style-type: none"> • DC1! (control state) • DC2! (output state) The MB-Data-Tags shall be presented in the RSP-UD (standard response) and in SND-NR (except static messages).	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41, Encryption and Authentication according to [OMS-S2], Table 39	

The new state of breaker / valve can be set by using described M-Bus command according to Table M.10.

Table M.10 – Requirements for OMS-UC-03; set control state

Functional	Wireless	Wired
Communication sequences unidirectional	N/A	N/A
Communication sequences bidirectional	Seq_SND-UDx [MBus-Cmd]	Seq_SND-UDx [MBus-Cmd]
Data elements to the OMS end-device	MB.Command-Tag: <ul style="list-style-type: none">• XDC1!	
Data elements from the OMS end-device	MB-Data-Tag: <ul style="list-style-type: none">• DC1! (control state)• DC2! (output state)	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41, Encryption and Authentication according to [OMS-S2], Table 39 Application security shall be applied with: <ul style="list-style-type: none">• ASP10 according to [OMS-S2], Table 44• BCF=20h/A0h acc. to [EN13757-7:2018], Table A.3• PID=01h acc. to [EN13757-7:2018], Table A.14• KeyID=20h• TargetTime set to "zero" (3000000000h) for immediate action; TargetTime for a delayed action can optionally also be supported ^a	
^a A not supported TargetTime value shall be replied with a SITP status response using value 23h, "Data structure content error: TargetTime error".		

M.2.5 OMS-UC-04 Clock Management

This use case describes the synchronisation of the clock of an OMS end-device, which can only be applied for bidirectional communicating OMS end-devices. It can be provided by adjusting or by absolute setting of the clock.

Both ways apply the Clock Synchronisation Protocol (see [OMS-S2], clause 8.7). The “Reserved” and “Command verification” fields of this protocol are optional and should be ignored in case they are provided.

Adjust Clock Time

The Adjust Clock Time command allows the device to correct the internal clock without time leaps and thus without the loss of time-controlled events. Time taken for adjustment of the clock depends on individual implementation, but shall be completed within 12 hours after reception of the Adjust Clock Time command. To validate the setting a readout after 12 hours is recommended.

As only one Adjust Clock Time command can be active, a further Adjust Clock Time command shall be not accepted as long as a previous adjustment is in process. In this case, an Adjust Clock Time command shall be ignored and replied with the Application error 10h (“Command cannot be executed at this time”).

Adjust Clock Time can use two parameter formats:

- “Time adjustment”
- “Time correction”

Time adjustment adds or subtracts a number of seconds. Therefore, it is necessary to request the current device time in advance for calculating the time deviation. For deviations up to ± 60 seconds (respectively ± 1 minute), the command processing shall be applied. Larger deviations shall not be accepted, the command shall be ignored and replied with the Application error 15h (“Parameter is missing or wrong”). This may lead to further time adjustment commands (after another 12 hours) until the desired time is reached.

Time correction provides an absolute time with the expected device time. This procedure is optimised for a broadcast approach. The OMS end-device has to calculate the deviation between the expected time and the current internal time. Only a maximum of ± 60 seconds (respectively ± 1 minute) shall be applied even if the calculated deviation is larger. This may lead to further time correction commands (after another 12 hours) until the desired time is reached.

NOTE: The maximum deviation of 60 seconds within 12 hours limits the maximum time variation.

The execution of the Adjust Clock Time command however shall not impact the synchronous transmission timing limits according to [OMS-S2], 4.3.2 and [EN13757-4:2019], 12.6.2.

The Adjust Clock Time command can be initiated either by the gateway or by the Head-End. Both variants provide different security levels. The gateway applies transport layer security only. The Head-End uses additional application layer security.

Set Date and Time

The Set Date and Time command allows the OMS end-device clock to be set to any desired time. It is seen as more critical than the Adjust Clock Time command and can only be provided by the Head-End with application layer security using a different key than the Adjust Clock Time command. An absolute setting of the OMS end-device’s clock shall be processed immediately and, if necessary, should stop a currently running Adjust Clock Time command.

Applicable Use Cases

Only one of the listed use cases shown in Table M.11 shall be active. The OMS end-device may offer several use cases to be selected by configuration. The respective use case number has to be provided in the ManDec.

Table M.11 – Requirements for OMS-UC-04; Allowed combinations of functions

Use case number	Function			
	Read Time	Adjust Clock Time by Gateway	Adjust Clock Time by Head-End	Set Date and Time by Head-End
OMS-UC-04a	X	X		
OMS-UC-04b	X	X	X	X
OMS-UC-04c^a	X		X	X
^a It shall be ensured that an OMS end-device providing “Adjust Clock Time by Head-End” does not accept a command “Adjust Clock Time by Gateway”.				

Table M.12 – Requirements for function “Read Time”

Functional	Wireless	Wired
Communication sequences unidirectional	Seq_SND-NR	N/A
Communication sequences bidirectional	Seq_SND-UDx [App-Reset, MBus-Data]	Seq_SND-UDx [App-Reset, MBus-Data]
Data elements to the OMS end-device	No requirements	
Data elements from the OMS end-device	MB-Data-Tag: <ul style="list-style-type: none"> DT1! The MB-Data-Tags shall be presented in the RSP-UD (standard response) and in SND-NR (except static messages).	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41, Encryption and Authentication according to [OMS-S2], Table 39	

Table M.13 – Requirements for function “Adjust Clock Time by Gateway”

Table 41: Requirements for function "Adjust Clock Time by Gateway"		
Functional	Wireless	Wired
Communication sequences unidirectional	N/A	N/A
Communication sequences bidirectional	Seq_SND-UDx [Clock-Sync]	Seq_SND-UDx [Clock-Sync]
Data elements to the OMS end-device	Clock Synchronisation Protocol according to [OMS-S2] 8.7, shall support both functions: <ul style="list-style-type: none">• "Time adjustment" (TC-field 01h or 02h and time format type J)• "Time correction" (TC-field 03h and time format type J)^a	
Data elements from the OMS end-device	No requirements	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41, Encryption and Authentication according to [OMS-S2], Table 39.	
^a This value is currently not covered by EN 13757-3:2018. TC = 03h defines a time correction with an absolute time applying CI-Field 6Dh. The use of "Reserved" and "Command verification" fields of EN 13757-3:2018 Table E.14 are optional.		

Table M.14 – Requirements for function “Adjust Clock Time by Head-End”

Functional	Wireless	Wired
Communication sequences unidirectional	N/A	NA/
Communication sequences bidirectional	Seq_SND-UDx [Clock-Sync]	Seq_SND-UDx [Clock-Sync]
Data elements to the OMS end-device	Clock Synchronisation Protocol according to [OMS-S2] 8.7, shall support both functions: <ul style="list-style-type: none">• “Time adjustment” (TC-field 01h or 02h and time format type J)• "Time correction" (TC-field 03h and time format type J)^a	
Data elements from the OMS end-device	No requirements ^d	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41, Encryption and Authentication according to [OMS-S2], Table 39. Application security shall be applied with: <ul style="list-style-type: none">• ASP10 according to [OMS-S2], Table 44• BCF=20h/A0h acc. to [EN13757-7:2018], Table A.3• PID=04h acc. to [EN13757-7:2018], Table A.14^c• KeyID=21h• TargetTime = 3000000000h (immediate action)^b	

^a This value is currently not covered by EN 13757-3:2018.
TC = 03h defines a time correction with an absolute time.

^b A not supported TargetTime value should be replied with a SITP status response using value 23h, “Data structure content error: TargetTime error”.

^c The APDU shall only consist of TC-Field and respective time format. The use of “Reserved” and “Command verification” fields of EN 13757-3:2018 Table E.14 are optional.

^d A SITP status response (DSI 22) shall be responded.

NOTE: The applied application security profile ensures that a command will be executed only once even if the message has been received several times (see EN13757-7:2018, A.9.1).

Table M.15 – Requirements for function “Set Date and Time by Head-End”

Table M10: Requirements for function "Set Date and Time by Head End"		
Functional	Wireless	Wired
Communication sequences unidirectional	N/A	N/A
Communication sequences bidirectional	Seq_SND-UDx [Clock-Sync]	Seq_SND-UDx [Clock-Sync]
Data elements to the OMS end-device	Clock Synchronisation Protocol according to [OMS-S2] 8.7, only function "Time setting" with TC-field 00h and time format type I shall be supported.	
Data elements from the OMS end-device	No requirements ^c	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41, Encryption and Authentication according to [OMS-S2], Table 39. Application security shall be applied with: <ul style="list-style-type: none">• ASP10 according to [OMS-S2], Table 44• BCF=20h/A0h acc. to [EN13757-7:2018], Table A.3• PID=04h acc. to [EN13757-7:2018], Table A.14 ^b• KeyID=22h• TargetTime = 3000000000h (immediate action) ^a	
^a A not supported TargetTime value should be replied with a SITP status response using value 23h, "Data structure content error: TargetTime error".		
^b The APDU shall only consist of TC-Field and respective time format. The use of "Reserved" and "Command verification" fields of EN 13757-3:2018 Table E.13 are optional.		
^c A SITP status response (DSI 22) shall be responded.		

NOTE 1: The function “Set Date and Time by HeadEnd” is mainly intended for devices, which may lose their date and time information during operation. It can also be used for initial time setting e.g. in a different time zone.

NOTE 2: The function “Set Date and Time by HeadEnd” may lead to imprecise time in the OMS end-device due to transmission delays of the command. The residual time deviation can be corrected by the function “Adjust Clock Time”.

M.2.6 OMS-UC-05 Firmware Update

This use case describes which message sequences will be used for transferring a new firmware to an OMS end-device. To this end, the image transfer protocol as specified in EN 13757-3:2018 Annex I will be used.

The image transfer consists of several phases. A prerequisite is that the new image is first uploaded from a HES system to the gateway and afterwards the gateway will transfer the new image to the OMS end-device. Here will only be described which message shall be used for the image transfer process between the gateway and the OMS end-device.

NOTE: Only the point-to-point Image transfer process is described, i.e. the gateway only transfers an image to one OMS end-device at a time and multicast is not used.

Tables for the different phases of the image transfer process are given in the following sections.

The state command and response can be used in any phase of the process to check the current status. The possible states are listed in EN 13757-3:2018 Table I.29. It is recommended to use it especially at the end of phase 2 to check the successful transmission.

Table M.16 – Requirements for OMS-UC-05; State Command & Response

Functional	Wireless	Wired
Communication sequences unidirectional	N/A	N/A
Communication sequences bidirectional	Seq_SND-UDx [ITP-Cmd, ITP-Rsp]	Seq_SND-UDx [ITP-Cmd, ITP-Rsp]
Data elements to the OMS end-device	State Command: See EN 13757-3:2018 Annex I, section I.2.11 <ul style="list-style-type: none"> • Function field 04h • Image Identifier Field: mandatory • Add. Info: optional. 	
Data elements from the OMS end-device	State Response: See EN 13757-3:2018 Annex I, section I.2.12 <ul style="list-style-type: none"> • Function field 84h • Image Identifier Field: mandatory 	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41. Encryption and Authentication shall be used according to [OMS-S2], Table 39.	

Phase 1: Transfer Preparation

The command sets up the condition for image transfer. The included MAC field allows securing the transmission of the image to the OMS end-device. The OMS end-device shall check the integrity of the image during the image validation step.

Table M.17 – Requirements for OMS-UC-05; Prepare Command & Response

Functional	Wireless	Wired
Communication sequences unidirectional	N/A	N/A
Communication sequences bidirectional	Seq_SND-UDx [ITP-Cmd, ITP-Rsp]	Seq_SND-UDx [ITP-Cmd, ITP-Rsp]
Data elements to the OMS end-device	Prepare Command: See EN 13757-3:2018 Annex I, section I.2.4 <ul style="list-style-type: none">• Function field 00h• Date and Time: shall not be used• Pace: shall not be used• Size information: mandatory^a• Image Identifier field: mandatory• MAC field: mandatory (ASP03 according to [OMS-S2], Table 44)<ul style="list-style-type: none">○ MAC Algorithm ID = 04h○ KeyID = 18h• Add. Info: optional	
Data elements from the OMS end-device	Prepare Response: See EN 13757-3:2018 Annex I, section I.2.5 <ul style="list-style-type: none">• Function field 80h• Image Identifier field: mandatory• Size Information: optional• Add. Info: optional	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41. Encryption/Authentication shall be used according to [OMS-S2], Table 39. Application security shall be applied with: <ul style="list-style-type: none">• ASP10 according to [OMS-S2], Table 44• BCF=20h/A0h acc. to [EN13757-7:2018], Table A.3• PID=06h acc. to [EN13757-7:2018], Table A.14• KeyID = 23h• TargetTime = 3000000000h (immediate action)^b	
^a The OMS end-device shall support a minimum block size of 190 bytes. Fragmentation by AFL is optional.		
^b A not supported TargetTime value should be replied with a SITP status response using value 23h, "Data structure content error: TargetTime error".		

Phase 2: Image Transfer

The transfer command is used for the actual transfer of the image. This phase consists of:

- Transferring the complete image from the gateway to the OMS end-device
- Checking the completeness of the image transfer and possibly retransferring missing blocks. This is an iterative process until all image blocks are successfully transferred
- Checking the state of the image transfer

Table M.18 – Requirements for OMS-UC-05; Transfer Command

Functional	Wireless	Wired
Communication sequences unidirectional	N/A	N/A.
Communication sequences bidirectional	Seq_SND-UD [ITP-Cmd]	Seq_SND-UD [ITP-Cmd]
Data elements to the OMS end-device	Transfer Command: See EN 13757-3:2018 Annex I, section I.2.7 <ul style="list-style-type: none"> • Function field 02h • Image Identifier Field: mandatory • Block number: mandatory • Remaining: optional • Add. Info: optional. 	
Data elements from the OMS end-device	Transfer Response: See EN 13757-3:2018 Annex I, section I.2.8 <ul style="list-style-type: none"> • Function field 82h • Image Identifier field: mandatory 	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41. Encryption and Authentication shall be used according to [OMS-S2], Table 39. To reduce the overhead by security elements a fragmentation of larger Image blocks is recommended. In order to ensure end-to-end security from manufacturer to OMS end-device it is recommended to additionally protect the image.	

The completion command is used to check if all the blocks of the image have been successfully transferred. In case the OMS end-device signals that there are blocks missing, the gateway must retransfer the missing blocks.

Table M.19 – Requirements for OMS-UC-05; Completion Command & Response

Functional	Wireless	Wired
Communication sequences unidirectional	N/A	N/A
Communication sequences bidirectional	Seq_SND-UDx [ITP-Cmd, ITP-Rsp]	Seq_SND-UDx [ITP-Cmd, ITP-Rsp]
Data elements to the OMS end-device	Completion Command: See EN 13757-3:2018 Annex I, section I.2.9 <ul style="list-style-type: none"> • Function field 03h • Image Identifier Field: mandatory • Add. Info: optional 	
Data elements from the OMS end-device	Completion Response: See EN 13757-3:2018 Annex I, section I.2.10 <ul style="list-style-type: none"> • Function field 83h • Image Identifier Field: mandatory • Total Number of lost blocks: mandatory • Lost Blocks field: shall only be present if Total Number of lost blocks > 0 	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41. Encryption and Authentication shall be used according to [OMS-S2], Table 39.	

NOTE: Since the transmission of each block was confirmed by the OMS end-device, the gateway may skip the completion check.

Phase 3: Image Validation

According to EN 13757-3:2018 Annex I, section I.1.5 the image validation is triggered by the AMMHES, and forwarded by the gateway to the OMS end-device.

Table M.20 – Requirements for OMS-UC-05; Validate Command & Response

Functional	Wireless	Wired
Communication sequences unidirectional	N/A	N/A
Communication sequences bidirectional	Seq_SND-UDx [ITP-Cmd, ITP-Rsp]	Seq_SND-UDx [ITP-Cmd, ITP-Rsp]
Data elements to the OMS end-device	Validate Command: See EN 13757-3:2018 Annex I, section I.2.13 <ul style="list-style-type: none"> • Function field 05h • Image Identifier Field: mandatory • Add. Info: optional. During this image validation step, the OMS end-device must recalculate the MAC value over the received image and compare this MAC value with the value received in the Prepare Command. Image validation is successful if both MAC values match and additional manufacturer tests are passed. Otherwise, the status will be “Validation failed”.	
Data elements from the OMS end-device	Validate Response: See EN 13757-3:2018 Annex I, section I.2.14 <ul style="list-style-type: none"> • Function field 85h • Image Identifier Field: mandatory 	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41. Encryption and Authentication shall be used according to [OMS-S2], Table 39.	

Phase 4: Image Activation

According to EN 13757-3:2018 Annex I, section I.1.6 the image activation is triggered by the AMMHES, and forwarded by the gateway to the OMS end-device. The device shall accept an activation command only if image validation in phase 3 has been finished with state “Validation successful”.

Table M.21 – Requirements for OMS-UC-05; Activate Command & Response

Functional	Wireless	Wired
Communication sequences unidirectional	N/A	N/A
Communication sequences bidirectional	Seq_SND-UDx [ITP-Cmd, ITP-Rsp]	Seq_SND-UDx [ITP-Cmd, ITP-Rsp]
Data elements to the OMS end-device	Activate Command: See EN 13757-3:2018 Annex I, section I.2.15 <ul style="list-style-type: none"> • Function field 06h • Image Identifier Field: mandatory • Date and Time: mandatory 	
Data elements from the OMS end-device	Activate Response: See EN 13757-3:2018 Annex I, section I.2.16 <ul style="list-style-type: none"> • Function field 86h • Image Identifier Field: mandatory 	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41. Encryption and Authentication shall be used according to [OMS-S2], Table 39. Application security profile should be applied with: <ul style="list-style-type: none"> • ASP10 according to [OMS-S2], Table 44 • BCF=20h/A0h acc. to [EN13757-7:2018], Table A.3 • PID=06h acc. to [EN13757-7:2018], Table A.14 • KeyID = 23h • TargetTime = 3080000000h (The Image Transfer Protocol provides an own “Date and Time” field for the image activation.) NOTE: In case Annex E.2 is supported by the OMS end-device, the Application security is not applicable by an IDIS gateway. Otherwise the application of ASP 10 is recommended.	

Optional messages: Terminate Command & Response

The terminate command is used to terminate the image transfer phase or to terminate the whole image transfer process.

Table M.22 – Requirements for OMS-UC-05; Terminate Command & Response

Functional	Wireless	Wired
Communication sequences unidirectional	N/A	N/A
Communication sequences bidirectional	Seq_SND-UDx [ITP-Cmd, ITP-Rsp]	Seq_SND-UDx [ITP-Cmd, ITP-Rsp]
Data elements to the OMS end-device	Terminate Command: See EN 13757-3:2018 Annex I, section I.2.17 <ul style="list-style-type: none">• Function field 07h• Image Identifier Field: mandatory	
Data elements from the OMS end-device	Terminate Response: See EN 13757-3:2018 Annex I, section I.2.18 <ul style="list-style-type: none">• Function field 87h• Image Identifier Field: mandatory	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41. Encryption and Authentication shall be used according to [OMS-S2], Table 39. Application security should be applied with: <ul style="list-style-type: none">• ASP10 according to [OMS-S2], Table 44• BCF=20h/A0h acc. to [EN13757-7:2018], Table A.3• PID=06h acc. to [EN13757-7:2018], Table A.14• KeyID = 23h• TargetTime = 3000000000h (immediate action) ^a NOTE: In case Annex E.2 is supported by the OMS end-device, the Application security is not applicable by an IDIS gateway. Otherwise the application of ASP 10 is recommended.	

^a A not supported TargetTime value should be replied with a SITP status response using value 23h, “Data structure content error: TargetTime error”.

M.2.7 OMS-UC-06 OMS End-device Supervision

Status information of the OMS end-device can be obtained by analysing the status Byte or by interpreting the data points error flags and/or battery lifetime. This use case explains how to get this information and how to clear respective error flags of the OMS end-device.

Table M.23 – Requirements for OMS-UC-06; get status information

Functional	Wireless	Wired
Communication sequences unidirectional	Seq_SND-NR	N/A
Communication sequences bidirectional	Seq_SND-UDx [App-Reset/App-Select, MBus-Data]	Seq_SND-UDx [App-Reset/App-Select, MBus-Data]
Data elements to the OMS end-device	No requirements	
Data elements from the OMS end-device	MB-Data-Tag: <ul style="list-style-type: none"> Error flag MM2! or MM3! (mandatory) Battery life time MM8! (optional). The status byte is always present in TPL. The MB-Data-Tags shall be presented in the RSP-UD (standard response) and in SND-NR (except static messages).	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41. Encryption and Authentication shall be used according to [OMS-S2], Table 39.	

There are two possibilities to clear status information. Either clear dedicated (bitwise) states or clear all possible states. It may not be possible to clear all errors as some can be permanent or the reason for the error is still present. The result can be checked in the command response where the respective data point will be delivered.

NOTE: Clearing a bit in data point error flags may also change the status byte whereas there is no chance to clear the status byte itself.

Table M.24 – Requirements for OMS-UC-06; clear status information

Functional	Wireless	Wired
Communication sequences unidirectional	N/A	N/A
Communication sequences bidirectional	Seq_SND-UDx [MBus-Cmd, MBus-Data]	Seq_SND-UDx [MBus-Cmd, MBus-Data]
Data elements to the OMS end-device	MB-Command: <ul style="list-style-type: none">notMM2! or notMM3! (clear bitwise)clrMM3! (clear all)	
Data elements from the OMS end-device	MB-Data-Tag: <ul style="list-style-type: none">MM2! or MM3!	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41. Encryption and Authentication shall be used according to [OMS-S2], Table 39. Application security shall be applied with: <ul style="list-style-type: none">ASP10 according to [OMS-S2], Table 44BCF=20h/A0h acc. to [EN13757-7:2018], Table A.3PID=01h acc. to [EN13757-7:2018], Table A.14KeyID=24hTargetTime = 3000000000h (immediate action) ^a	
^a A not supported TargetTime value should be replied with a SITP status response using value 23h, "Data structure content error: TargetTime error".		

M.2.8 OMS-UC-07 Consumer Information

This use case describes how an M-Bus OMS end-device shall provide additional consumer information over wireless or wired M-Bus. It declares in Table M.27 the mandatory data elements dependant on the device type.

This use case can be applied for both unidirectional and bidirectional OMS end-devices. For unidirectional devices the data are provided only with SND-NR message.

According to [OMS-S1], 4.3 the consumer information can be provided by the AMM-HES, the gateway or directly from the related OMS end-device. The last type of communication uses a different TPL-key with a different KeyID.

The master key is used by the MSO for the data exchange between the OMS end-device and the gateway or AMM-HES. It should not be shared in devices that are not under the control of the MSO.

The OMS end-device shall support one or both of the sub use cases shown in Table M.25.

Table M.25 – Sub use cases for OMS-UC-07

Sub use case	KeyID	Possible scenario
UC-07a	00h	Consumer information is sent to the gateway or AMM-HES for further processing and then forwarded to a display unit or comparable.
UC-07b	08h	Consumer information is sent directly to the display unit (the gateway may be used as a relay).

Figure 2 depicts possible scenarios for the data transfer from the OMS end-device via gateway or AMM-HES.

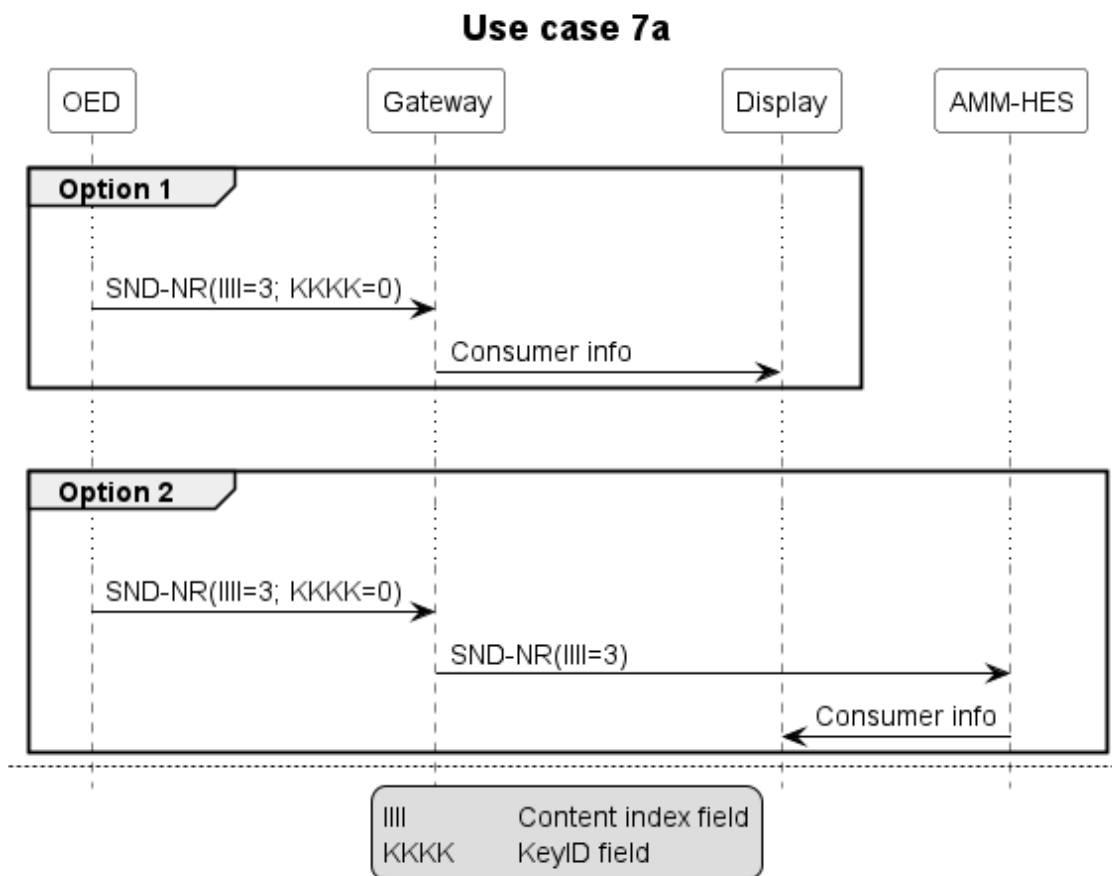


Figure 2 – Scenarios for the data transfer to the display via gateway or AMM-HES

Figure 3 depicts possible scenarios for the data transfer from the OMS end-device to the display.

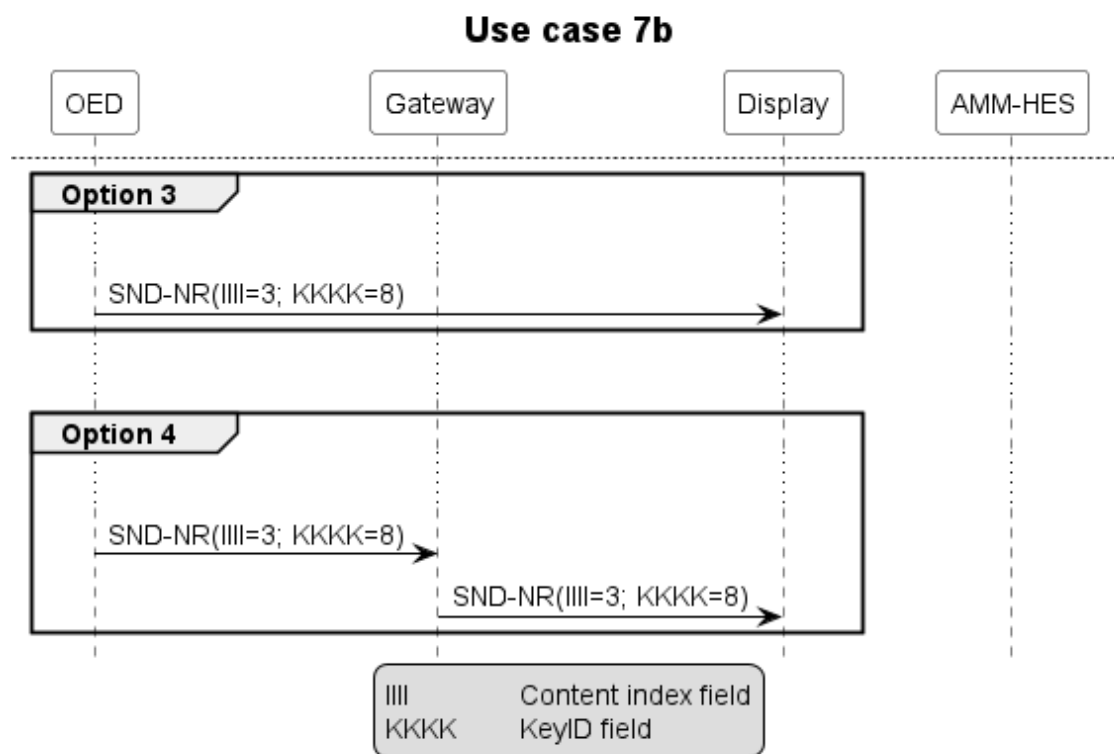


Figure 3 – Scenario for the direct data transfer to the display

To allow the gateway or the display unit to identify the datagrams with consumer information a special content index is used (see [OMS-S2], 7.2.4.7). Based on this content index field the gateway may filter this datagram or forward it to a display unit or the AMM-HES.

NOTE : If security profile C is applied for use case 7b a service of the MSO (as owner of the OMS end-device) is necessary to establish a secure connection. The key needs to be provided to the display owner that has to insert it to the display. This service is needed every time a new display is installed.

Table M.26 – Requirements for OMS-UC-07, get consumer information

Table M.25 Requirements for OMS SS-01, get consumer information		
Functional	Wireless	Wired
Communication sequences unidirectional	Seq_SND-NR	n.a.
Communication sequences bidirectional	Seq_SND-UDx [App-Select, MBus-Data]	Seq_SND-UDx [App-Select, MBus-Data]
Data elements to the OMS end-device	Select message application 18 (see [OMS-S2], 8.10)	
Data elements from the OMS end-device	<p>The OMS end-device shall provide the MB-Data-Tags according to Table M.27.</p> <p>The MB-Data-Tags shall be present in the RSP-UD (message application 18) and in SND-NR datagrams for consumer information that shall be marked according to [OMS-S2], 7.2.4.7.</p> <p>These SND-NR datagrams for consumer information shall be transmitted at least every 15 minutes (respecting tolerances according to [OMS-S2], 4.3.2.2). Electricity meters shall provide these SND-NR every 7,5 minutes.</p> <p>Resolution of meter indexes and/or instantaneous power or flow rate for consumer feedback shall be according to CEN/TR 17167 Annex C. Thus, a receiver is able to calculate, reasonable consumption values (e.g. flow values).</p>	
Security requirements	<p>Selection of Security profile according to [OMS-S2], Table 41, except “no security profile” and Security profile A^a.</p> <p>The KeyID of SND-NR datagrams for consumer information shall be applied according to Table M.25.</p>	
^a Both security profiles do neither provide the necessary KeyID subfield nor context index subfield.		

Table M.27 – Requirements for OMS-UC-07, mandatory data elements

Device	Dev.-Type	MB-Data Tag	Description
Electricity	02h	EW1!	(Active) energy import
		EW1!R	Active energy import, recent value for billing
		EW2!	Active energy export (only if available)
Heat Cost Allocator	08h	DT2!D	Local date at due date
		HC1!	Unrated integral, current value
		HC1!D	Unrated integral, due date value
Cooling, Heat	0Ah, 0Bh, 04h, 0Ch	DT2!D	Local date at due date
		EJ1!, EW1! ^a	Energy import
		EJ1!D, EW1!D ^a	Energy import, due date value
		TC1!	Flow temperature, current value
		TC2!	Return temperature, current value
Heat/Cooling	0Dh	DT2!D	Local date at due date
		EJ1!, EW1! ^a	Energy import (1st value for heat)
		EJ1!T, EJ2!, EW1!T, EW2! ^a	Energy import (2nd value for cooling)
		EJ1!D, EW1!D ^a	Energy import (1st value for heat), due date value
		EJ1!DT, EW1!DT, EJ2!D, EW2!D ^a	Energy import (2nd value for cooling), due date value
		TC1!	Flow temperature, current value
		TC2!	Return temperature, current value
Gas	03h	VM1!, VM2!, VM3! ^a	Volume, current value, total
Water, Hot Water	06h, 07h, 16h, 28h, 15h	DT2!D	Local date at due date
		VM1!	Volume, current value, total
		VM1!D	Volume (V), accumulated, total, due date value
Breaker, Valve ^b	20h, 21h	DC1!	Current state of breaker/valve
^a At least one of the MB-Data Tags shall be provided.			
^b All devices with a breaker or valve function shall provide this data point.			

M.2.9 OMS-UC-08 Key Management

This use case describes how to change a key in a wired or wireless OMS end-device.

The key management is separated into two different steps.

1. Transfer of new keying material to the OMS end-device.
2. Activate new key and deactivate old key.

The remote key management process requires wrapper keys (WK) in the OMS end-device. This wrapper key must be provided to the OMS end-device and to the operator prior to executing this use case.

All necessary commands for the key management shall use the Security Information Transfer Protocol (according to [EN 13757-7:2018], Annex A). The SITP can only be applied for bidirectional communicating OMS end-devices.

To exchange a key at least the second step shall be performed. The first step may be skipped, if new keying material is already available in the OMS end-device (preloaded in the factory).

The exchange of the master key needs some special treatment as it affects the transport security. Appendix M.A (informative) shows the message flow between the Head End, the Gateway and the OMS end-device for all three steps of master key renewal.

Note 1: If the gateway (or the operator) is not aware of the currently used keying material, the SITP can also be used to get a list of active key information. The current key version of the master key can be requested by the gateway with activating the AFL.KI flag in any command (see [OMS-S2], 6.2.2).

Note 2: If a key exchange is requested with an older key version than the current one, then the OMS end-device may refuse the key renewal.

Table M.28 – Requirements for OMS-UC-08; Get list of keys

Table A.12 – Requirements for OMS-S2-S3, Set list of keys		
Functional	Wireless	Wired
Communication sequences unidirectional	N/A	N/A
Communication sequences bidirectional	Seq_SND-UDx [SITP-Cmd, SITP-Rsp]	Seq_SND-UDx [SITP-Cmd, SITP-Rsp]
Data elements to the OMS end-device	Command “Get list of active key information”: <ul style="list-style-type: none">BCF = 08h acc. to [EN13757-7:2018], Table A.3 Command “Get list of active keys and key counter information”: <ul style="list-style-type: none">BCF = 09h acc. to [OMS-S2], Annex F, F.A.5	
Data elements from the OMS end-device	Response “Get list of active key information”: <ul style="list-style-type: none">BCF = 88h acc. to [EN13757-7:2018], Table A.3DSI = 21h acc. to [EN13757-7:2018], Table A.5^b Response “Get list of active keys and key counter information”: <ul style="list-style-type: none">BCF = 89h acc. to [OMS-S2], Annex F, F.A.5^aDSI = 23h acc. to [OMS-S2], Annex F, Table F.A.5^{a, b}	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41. Encryption and Authentication according to [OMS-S2], Table 39. Application security shall be applied with: <ul style="list-style-type: none">ASP01 according to [OMS-S2], Table 44BCF according to the data elements	
^a This value is currently not covered by EN 13757-3:2018. ^b Or DSI = 22h in case of an error		

Table M.29 – Requirements for OMS-UC-08; Transfer of keying material

Functional	Wireless	Wired
Communication sequences unidirectional	N/A	N/A
Communication sequences bidirectional	Seq_SND-UDx [SITP-Cmd, SITP-Rsp]	Seq_SND-UDx [SITP-Cmd, SITP-Rsp]
Data elements to the OMS end-device	Command “Transfer security information”: <ul style="list-style-type: none"> • BCF = 00h acc. to [EN13757-7:2018], Table A.3 • DSI = 01h acc. to [EN13757-7:2018], Table A.5 • DSH1 = KeyID 10h to 15h acc. to [OMS-S2], 9.2.2 • DSH2 = KeyVersion of DSH1 KeyID • Data structure content: <ul style="list-style-type: none"> ○ “Key” is the transferred key (acc. to [EN13757-7:2018], A.8.3). ○ “Target Time” = 3080000000h (Setting “invalid” in order to avoid immediate key activation.) ○ “Key ID” is the KeyID of the transferred key ○ “Key Version” is the KeyVersion of the transferred key, KeyVersion shall be managed by AMMHES. This means KeyVersion = FFh is not allowed. 	
Data elements from the OMS end-device	Response “Transfer security information”: <ul style="list-style-type: none"> • BCF = 80h acc. to [EN13757-7:2018], Table A.3 • DSI = 22h acc. to [EN13757-7:2018], Table A.5 	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41. Encryption and Authentication according to [OMS-S2], Table 39. Application security shall be applied with: <ul style="list-style-type: none"> • ASP01 according to [OMS-S2], Table 44 	

Table M.30 – Requirements for OMS-UC-08; Activation/Deactivation of keying material

Functional	Wireless	Wired
Communication sequences unidirectional	N/A	N/A
Communication sequences bidirectional	Seq_SND-UDx [SITP-Cmd, SITP-Rsp]	Seq_SND-UDx [SITP-Cmd, SITP-Rsp]
Data elements to the OMS end-device	Command “Combined activation/deactivation of security information”: <ul style="list-style-type: none"> • BCF = 04h acc. to [EN13757-7:2018], Table A.3 • DSI = 03h acc. to [EN13757-7:2018], Table A.5 • DSH1 = KeyID 10h to 15h acc. to [OMS-S2], Table 39 • DSH2 = KeyVersion of DSH1 KeyID • Data structure content: <ul style="list-style-type: none"> ○ “Target Time” = 3000000000h (immediate action) ○ “Activated Key ID” shall be set acc. to [OMS-S2], 9.2.3 ○ “Activated Key Version” is the version number of the new key to be activated ○ “Deactivated Key ID” shall be identical to “Activated Key ID” ○ “Deactivated Key Version” is the version number of the currently active key ○ “Option” shall be set to 1 in case of KeyID=00h (MK) to perform the message counter reset of CM. ○ “Option” should be set to 1 in case of KeyID>=10h to perform the key counter reset. 	
Data elements from the OMS end-device	Response “Combined activation/deactivation of security information”: <ul style="list-style-type: none"> • BCF = 84h acc. to [EN13757-7:2018], Table A.3 • DSI = 22h acc. to [EN13757-7:2018], Table A.5 	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41. Encryption and Authentication according to [OMS-S2], Table 39. Application security shall be applied with: <ul style="list-style-type: none"> • ASP01 according to [OMS-S2] Table 44 • BCF according to the data elements 	

M.2.10 OMS-UC-12 Application Management

M.2.10.1 Overview

This use case describes message sequences that shall be used to manage the settings in an OMS end-device. The following management functions are harmonised in OMS:

Table M.31 – Harmonised configuration functions

Sub use case	Function
OMS-UC-12a	Due date management
OMS-UC-12b	Customer ownership number

M.2.10.2 OMS-UC-12a Due Date Management

UC-12a describes three functions:

- request the last due date of an OMS end-device
- request the next due date of an OMS end-device
- set the next due date of an OMS end-device

Note: The set-function does **not** provide possibilities to define functional details like:

- the type of the due date (e.g. half yearly)
- The time when to store the values (e.g. 00:00 o clock)
- Time-zone and daylight-saving-time

Table M.32 – Requirements for OMS-UC-12a; Get last due date

Functional	Wireless	Wired
Communication sequences unidirectional	N/A	N/A
Communication sequences bidirectional	Seq_SND-UDx [M-Bus]	Seq_SND-UDx [M-Bus]
Data elements to the OMS end-device	MB-Command Tag: <ul style="list-style-type: none"> • Get last due date (getDT2!D) 	
Data elements from the OMS end-device	MB-Data Tag: <ul style="list-style-type: none"> • Local date at last due date (DT2!D) 	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41. Encryption and Authentication shall be used according to [OMS-S2], Table 39.	

Table M.33 – Requirements for OMS-UC-12a; Get next due date

Functional	Wireless	Wired
Communication sequences unidirectional	N/A	N/A
Communication sequences bidirectional	Seq_SND-UDx [M-Bus]	Seq_SND-UDx [M-Bus]
Data elements to the OMS end-device	MB-Command Tag: <ul style="list-style-type: none"> Get next due date (getDT2!N) 	
Data elements from the OMS end-device	MB-Data Tag: <ul style="list-style-type: none"> Local date at next due date (DT2!N) 	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41. Encryption and Authentication shall be used according to [OMS-S2], Table 39.	

Table M.34 – Requirements for OMS-UC-12a; Set next due date

Table 10: Requirements for OMS SS 12a, set next due date		
Functional	Wireless	Wired
Communication sequences unidirectional	N/A	N/A
Communication sequences bidirectional	Seq_SND-UDx [MBus-Cmd]	Seq_SND-UDx [MBus-Cmd]
Data elements to the OMS end-device	MB-Command Tag: <ul style="list-style-type: none">Set next due date (setDT2!N) ^a	
Data elements from the OMS end-device	MB-Data Tag: <ul style="list-style-type: none">Local date at next due date (DT2!N)	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41, Encryption and Authentication according to [OMS-S2], Table 39. Application security shall be applied with: <ul style="list-style-type: none">ASP10 according to [OMS-S2], Table 44BCF=20h/A0h acc. to [EN13757-7:2018], Table A.3PID=01h acc. to [EN13757-7:2018], Table A.14KeyID=26h according to [OMS-S2], Table 42TargetTime shall be set to "zero" (3000000000h) for immediate action	
^a The due date shall be a valid date in the future. Wildcards like every day and every month are not supported.		

M.2.10.3 OMS-UC-12b Customer Ownership Number

The ownership number is a modifiable alphanumeric number that is intended to optimize the customer's process management. It is optionally provided by a meter/actuator. OMC-UC-12b describes two functions to request and set the ownership number of a meter/actuator.

Table M.35 – Requirements for OMS-UC-12b; Get ownership number

Functional	Wireless	Wired
Communication sequences unidirectional	n.a.	n.a.
Communication sequences bidirectional	Seq_SND-UDx [MBus-Cmd]	Seq_SND-UDx [MBus-Cmd]
Data elements to the meter/actuator	MB-Command-Tag: <ul style="list-style-type: none"> getID4! 	
Data elements from the meter/actuator	MB-Tag: <ul style="list-style-type: none"> ID4! 	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41. Encryption and Authentication shall be according to [OMS-S2], Table 39.	

Table M.36 – Requirements for OMS-UC-12b; Set ownership number

Functional	Wireless	Wired
Communication sequences unidirectional	n.a.	n.a.
Communication sequences bidirectional	Seq_SND-UDx [MBus-Cmd]	Seq_SND-UDx [MBus-Cmd]
Data elements to the meter/actuator	MB-Command-Tag: <ul style="list-style-type: none"> setID4! 	
Data elements from the meter/actuator	MB-Tag: <ul style="list-style-type: none"> ID4! 	
Security requirements	Selection of Security profile according to [OMS-S2], Table 41. Encryption and Authentication shall be according to [OMS-S2], Table 39. Application security shall be applied with: <ul style="list-style-type: none"> ASP10 according to [OMS-S2], Table 44 BCF= 20h/A0h acc. to [EN13757-7:2018], Table A.3 PID = 01h acc. to [EN13757-7:2018], Table A.14 KeyID = 26h according to [OMS-S2], Table 42 TargetTime shall be set to "zero" (3000000000_h) for immediate action 	

M.2.11 OMS-UC-14 Data Selection

This use case is used to select the data requested from the Meter device.

UC-14 describes these functions:

- Modify readout-list of a message application

Note: With the selection of special applications the content of the SND-NR – transmissions can be modified too. See [OMS-S2], 8.10 for details.

Table M.37 – Requirements for OMS-UC-14; Data point selection

Functional	Wireless	Wired
Communication sequences unidirectional	n.a.	n.a.
Communication sequences bidirectional	Seq_SND-UDx [MBus-Cmd, MBus-Data]	Seq_SND-UDx [MBus-Cmd, MBus-Data]
Data elements to the meter/actuator	<p>MB-Command Tag:</p> <ul style="list-style-type: none">• Address application (setMM6!) ^a AND<ul style="list-style-type: none">○ EITHER Add data point to readout-list (arlXXX!) ^b○ OR Delete data point from readout-list (drlXXX!) ^b <p>Where XXX is any MB-data-tag as specified in [OMS-S2], Annex B, but with data field = 0_h (“no data”) and action code for arl or drl according to B1.4.</p> <p>The command setMM6! shall be placed prior to the commands arlXXX! or drlXXX! in the message.</p>	
Data elements from the meter/actuator	<p>In case of successful command execution, the response contains all data points of the selected application and the selected block number including the MB-data-tag MM6!.</p> <p>If the command has attempted to add or delete unimplemented data points, they shall be ignored by the meter/actuator. The response contains all accepted data points of the selected application and the selected block number including the MB-data-tag MM6!</p> <p>In case the L-Field would overflow or any other datagram length limit would exceed, a general application error with an error code 03_h (“Record overflow”) acc. to [OMS-S2], 8.8, Table 35, is responded.</p>	
	<p>Selection of Security profile according to [OMS-S2], Table 41, Encryption and Authentication according to [OMS-S2], Table 39.</p> <p>Application security shall be applied with:</p> <ul style="list-style-type: none">• ASP10 according to [OMS-S2], Table 44• BCF=20h/A0h acc. to [EN13757-7:2018], Table A.3• PID = 01h acc. to [EN13757-7:2018], Table A.14• KeyID=25h according to [OMS-S2], Table 42	

^a This data-tag contains the currently selected message application and block number according to [EN 13757-3:2018], 7.2.

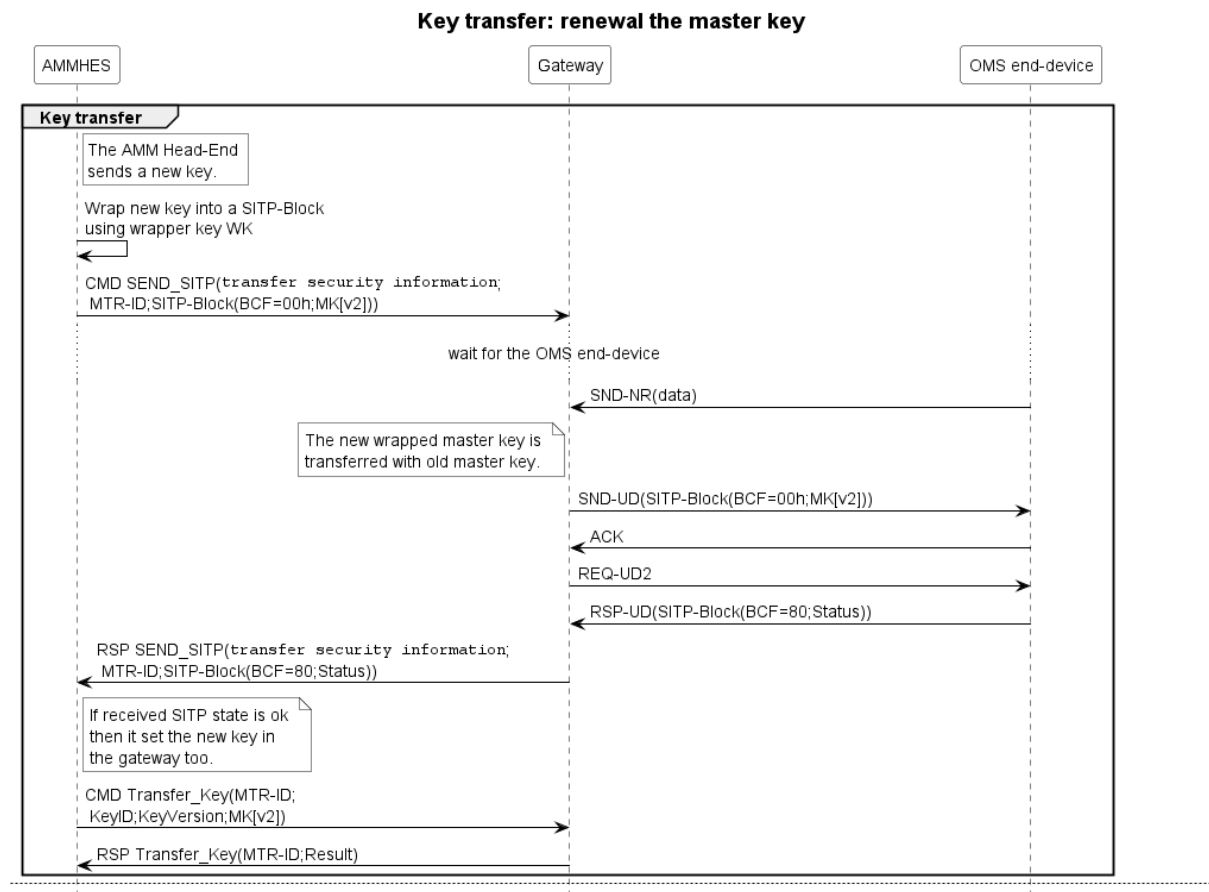
^b It is allowed, but not required to add more than one arlXXX or drlXXX in a message.

Table M.38 – Example for data point selection in Application 7, block 0

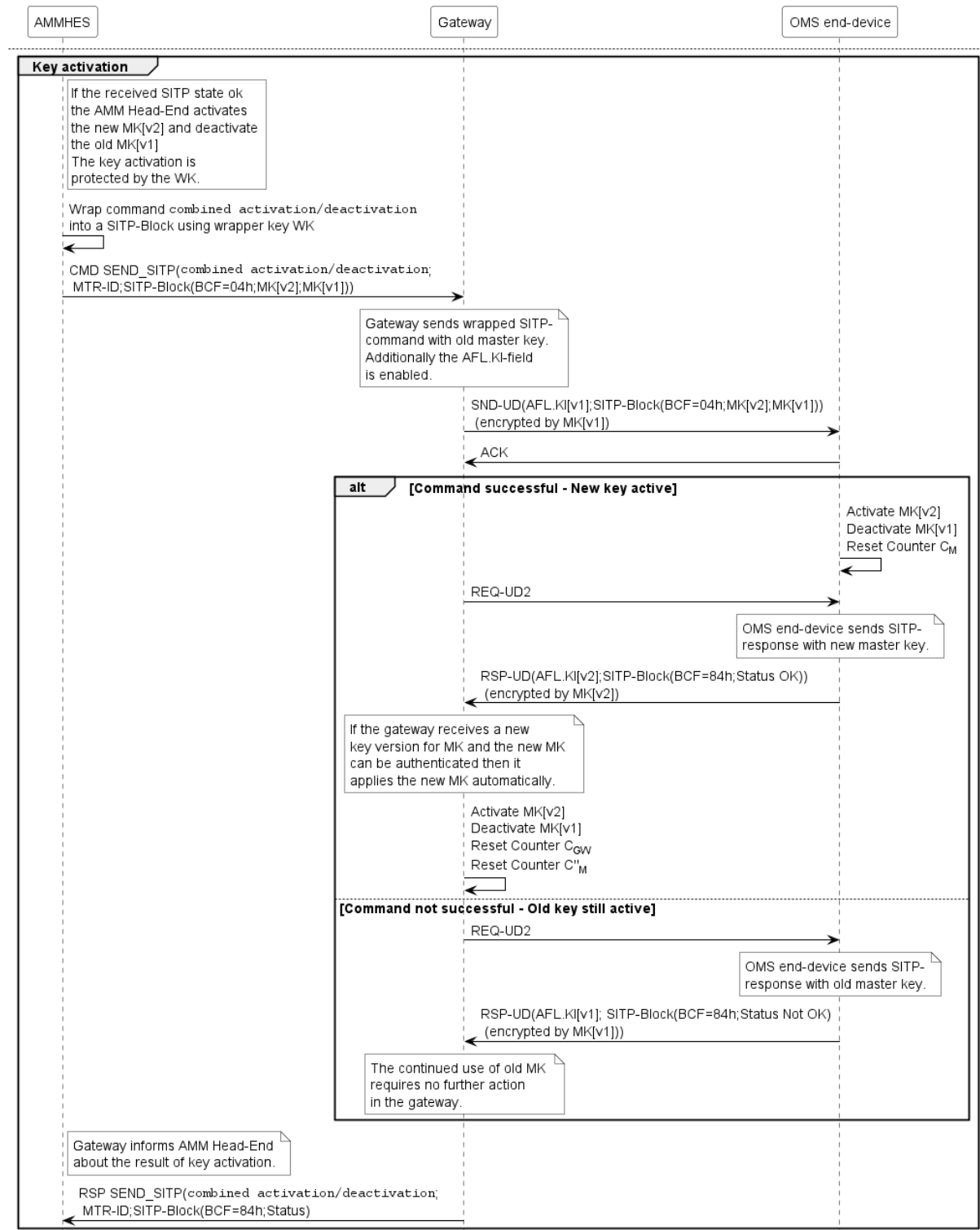
MB-Command Tags	M-Bus data points	Explanation
setMM6! + arlDP3!	01 FD FD 80 00 70 00 FD BC 0C	Application selection and Data point selection in one command sequence
setMM6! + arlDP3! + drlMM8! + arlMM4!	01 FD FD 80 00 70 00 FD BC 0C 00 FD F4 0D 00 FD AA 0C	Application selection and two Data points added and one data point removed in one command sequence. The support of more than one Data point selection is optional.

Appendix M.A (informative)

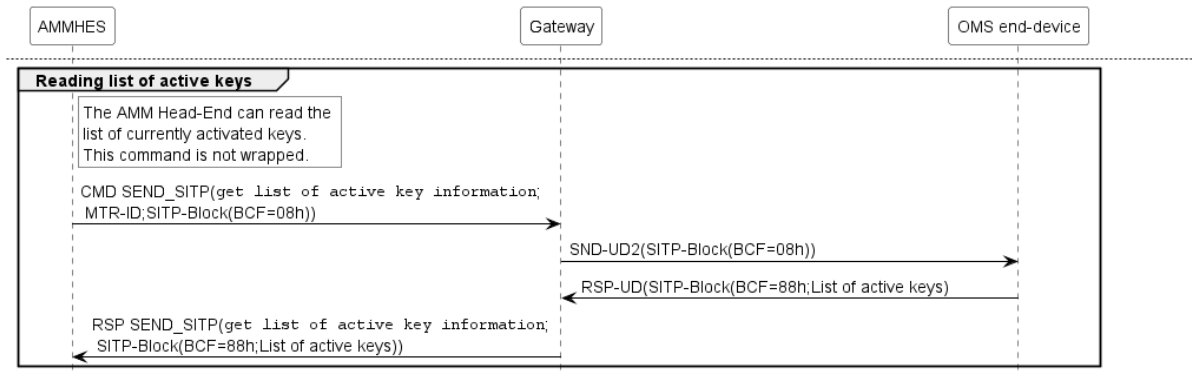
Example for the Renewal of the Master Key OMS-UC-08



Key activation of the new master key



Reading list of active keys



Key destruction of the old master key

