Open Metering System Specification

Volume 2
Primary Communication

Issue 5.0.1 / 2023-12

RELEASE

Document History

Version	Date	Comment	Editor
1.0.0	2008-06-27	First final Version	U. Pahl
1.0.1	2008-07-01	Editorial Revision	U. Pahl
1.0.2	2008-07-21	Some format adoptions; table index added; content index limited to structure level 3.	H. Baden
1.0.3	2009-02-25	Correct mistake in Table 10 Add changes for 2nd Version	U. Pahl
1.0.4	2009-05-13	Revision in AG1	AG1
1.0.5	2009-05-30	Add changes for 2nd Version	U. Pahl
1.0.6	2009-06-11	Update Annex	U. Pahl
1.0.7	2009-06-30	Changes based on protocol#23	U. Pahl
1.0.8	2009-07-03	Last changes of online review; update Annex A;,L and M, editorial review	U. Pahl
1.0.8	2009-07-05	Editorial and formal review	H. Baden
1.0.9	2009-07-17	Add Time sync frame to MUC-Status, separate ACC-No for wired M-Bus and wireless M-Bus	U. Pahl
2.0.0	2009-07-20	Release as V2.0.0	U. Pahl
2.0.1	2010-04-10	Add Changes for 3rd Version, Add sync Meter transmission; New CI-Fields	U. Pahl
2.0.2	2010-11-05	Add Compact M-Bus Profile; Harmonise Spec. with [prEN 13757-3]/[prEN 13757-4]	U. Pahl
2.0.3	2010-11-17	Revision in AG1	AG1
2.0.4	2010-12-17	Comments from members of AG1, Bug fix in Annex B	U. Pahl
3.0.0	2011-01-21	Update Changes from Standard revision	U. Pahl
3.0.1	2011-01-28	Editorial Revision. Release as V3.0.1	U. Pahl / A. Bolder
4.0.0	2013-01-10 2013-05-06 2013-07-02 2013-08-19 2013-08-30 2013-09-24 2013-10-20 2013-10-21 2013-10-23	New Introduction; Add BSI-support (AFL; new Encryption Mode 7 (dyn. AES) and Mode 13 (TLS); restructure chapters "Supported Device Types" and "Application protocols"; Revision of OBIS-List format; Add new M-Bus Datapoint list, add new section Address handling; Add mandatory support of ELL, Add Mode C support, Remove obsolete Annex E,F and M; general editorial revision, Add new ext. Annex B, E,F,O and int Annex J; Change Annex A to ext. Annex A; expand rules for ELL-Access number and TPL-Access number Add Timing Diagram fragm. SND-UD	U.Pahl / A. Bolder
4.0.1	2014-01-18	Changes according to Enquiry comments (see OMS_KommentareVol2Issue4_sortiert2_bearbAG1.doc)	U.Pahl
4.0.2	2014-01-27	Add Note to Annex G; Rename VIF-Type to VIB-Type Version 4.0.2 is released	U.Pahl
4.1.0	2016-02-10	Editorial revisions like Decimal-comma; Update Terms "serial number, manufacturing number, DIN-Fabrication number; New chapter 3.3 "Address handling by Adapters"; 4.1: Rename Title "Twisted Pair Connection (M-Bus)"; 4.2.3.2: Ed. Revision + del. Footnote c in Tab.9; Tab.10: Ignore FCB in wireless M-Bus; Tab.10+Tab.11+Tab.28: add NACK; 5.1+5.2.1+5.2.4 min. datagram length; 6.2.6 Msg. counter initialisation with 0; 7.2.2.1 FCB vs ACC-No; 7.2.3 clearing of bits “any application error”; Tab.22 Bit23 set to 0_b; 7.2.4.3 Add explanation for bits C,B,A,S,R,H,N; 7.2.4.4 Add explanation for bits N; 7.2.4.4/7.2.4.5 Notes about ELL-usage for wireless M-Bus only;	U.Pahl

Version	Date	Comment	Editor
4.1.0 (cont.)	2016-03-07	4.2.2.4 sync. transmission of static messages 4.2.3.1 tRO_slow in C2-Mode 7.2.3+Annex D Update applicable CI-Fields 8.2.6 new chapter "Descriptors" Annex K - new annex "Descriptors" 8.6 reset of Appl. Errors 8.6 Appl. Errors unencrypted 9.1 Encryption of protocols and M-bus data points; Byte order of keys Tab28: Default value AT/ATO 9.4.4 techn.revision of message counter 9.4.7 ed.revision of Key-calc Tab.G4 Bug fix in column "hex coded" Tab.1 Add CI=54h,55h,66h,67h,68h Application Select Protocol	U.Pahl
	2016-06-13	Editorial Changes according to "20160616_OMS_Table4Comments_OMSS410.docx" Change term "dynamic key" to "ephemeral key" Change term "static key" to "persistent key" 1.2 update of version history 3.1.3.2 case 1) ELLA check by other device 4.1, 5.2.1, 8.2.1, 9.2.1 5.2.3.1 Add new headline "General" Move 4.2.2 (without subclauses 4.2.2.1-4.2.2.4) to a new sub section 4.3.2.5 "Minimum time delay" Move headline 8.1.1. to 8.1 and replace old headline 8.1 "General Requirements" 5.2.4 and 8.5 add exception of clock service 6.2.3 FID for unfragmented messages 6.2.4; 6.2.7, 9.1; 9.3.1 merge 2 bit fields AT and ATO to a 4 bit AT-field Move AFL.ML from 6.2.5 to 6.2.8 Add new 6.2.5 AFL.KI 7.1 Rename combined Transport/Application layer to Transport layer to follows new structure of [EN 13757-7] and [EN 13757-3] Moving parts of subclause 7.1 to new subclause "8.1 Overview" 7.2.1; 7.2.4; Annex D: split CF in CF + CFE 7.2.4.4 Tab.22 update reserved fields; 7.2.4.4 Tab.23 extend KeyID to 4 bit 7.2.4.6 Tab.26+Tab.27 Signed data message was withdrawn, Reserved values were updated Extend Annex B with Enc.-requirements Annex C update M-Bus-Master requirements	
	2016-06-13	Update Annex J Annex L: Adding Headlines L.1-L.8 Annex L.4 review Example with NACK Bug Fix Annex N Change Term "Encryption Mode" by "Security Mode" Add new Subclause "8.8 Security Management Protocol" and add CI-Fields C3h-C5h in Tab.1	
	2016-06-23	Add new subclause 9.4 KeyID Replace Annex L.8 by inst. procedure w/o repeater	
4.1.1	2016-09-16	3.1.3.2 new condition to apply ELLA 5.2.3 Tab11 new footnote d (SND-NKE) 6.2.5 Revision AFL-KI Annex G.2 Update exceptions	U.Pahl
	2016-10-21	9.1 update definition of persistent and ephemeral key 7.3 update Tab.29 add reference/optional TPL for NACK	

Version	Date	Comment	Editor
4.1.2	2016-12-16	9.3.2 update according to comments from BSI 9.1 Tab.30: add Footnote b Annex F: update Introduction Annex G: Rename title to "Conversion of a Load Profile to single data points" Version v4.1.2 was released!	U.Pahl
4.2.0	2019-09-20	1.3 chapter added 2.2 Tab. 1: CI fields added and changed 3.1.4 reference updated 4.3.1 new note 4.3.2.3 new reference, addition of 60 s interval 4.3.3.1, Tab. 9 changed 4.3.4 changed 5.2.5 changed 6 complete chapter optimized for standard references 7.2.3 changed 8.1 bullet point added 8.2 complete chapter added 8.4.4 paragraph added 8.4.7 changed 8.4.8 complete chapter added 8.6 changed 8.9 chapter added 9 chapter content and structure completely revised 9.1 Tab. 33 updated, column authentication added, Tab. 34 and 35 changed Annexes A, B, E, F, H, J, K changed Annex L: changed to “informative”, drawings updated Annex M added Standard references updated Editorial revision	AG1, A. Reissinger
4.2.1	2019-11-23	Release version	A. Reissinger
4.3.0	2019-12-17 and 2020-01-06	2.3 Tab. 3 changed 4.2.1 chapter added for new Annex P 4.2.2 last sentence deleted 5.1 chapter changed for new Annex P, last sentence in first paragraph deleted 9.2.2 Tab. 38 corrected Annex C content deleted	AG4, A. Reissinger
4.3.1	2020-03-19 and 2020-05-04 and 2020-05-26 to 2020-05-29	Annex P page revised Tab. 15, 33, 34 and 36 changed Fig. 15 changed 8.2.5 changed 8.8 changed “meter(s)/actuator(s)” replaced with “meter” in all locations 8.1 changed, tab. 25 added 8.4.5.1 new paragraph added Tab. 1 changed 9.3.2 chapter structure fixed	AG4, A. Reissinger AG1, A. Reissinger AG1, A. Reissinger
4.3.2	2020-06-29 to 2020-07-09	1.2 changed Tab. 2 and 3 changed Tab. 39 changed Release candidate	A. Reissinger

Version	Date	Comment	Editor
4.3.3	2020-09-24 and	8.4.4 changed 9.2.3 changed 9.4.2.1 changed Annex L.5 updated	AG1, A. Reissinger
	2020-09-29 and	3.2 changed 8.4.5.2 changed	U. Pahl, T. Banz
	2020-10-02 and	Editorial changes	A. Reissinger
	2020-10-13 and	Integration of several action items: Introduction of Annex M changed 5.2.5 changed	AG1, A. Reissinger T. Banz
	2020-10-22	Editorial changes Release	A. Reissinger
4.4.0	2021-09-08	Table 13: headline corrected 1.1, 1.2 changed: introduction of sensors Tables 2 and 4 changed: introduction of sensors Annex C: reference to new external Annex C added	T. Banz, A. Reissinger D. Matussek R. Müller A. Reissinger
4.4.1	2021-09-15 and	Table 24 changed	A. Reissinger
	2021-09-29 and	Editorial changes	D. Matussek, A. Reissinger
	2021-10-21	Release candidate	A. Reissinger
4.4.2	2021-12-01	9.2.3 added Table 23: Title and headline changed Editorial changes Release	AG1, A. Reissinger

Version	Date	Comment	Editor
4.5.0	2022-01-31	4.3.2.2, 4.3.2.3 and 4.3.2.4 changed 7.2.4.4 and 7.2.4.6 changed 7.2.4.7 added 8.4.4 changed Table 39 changed Figure 16 changed	AG1, A. Reissinger
	2022-02-10	Headline of clause 9.3.2.3 edited	
	2022-02-24	2.3 changed Table 38: footnote added	
	2022-03-18	2,3 changed 4.3.2.4 changed 8.4.4 changed Table 2 changed Table 22 headline changed Table 36 headline and note changed	
	2022-06-10	Copyright remark added to front page	
	2022-07-05	Editorial changes on front page	
	2022-07-25	Table 1 changed (network management) Table 24 changed (network management) Tables 37 and 39 changed (transport key) 9.2 changed (transport key) 9.3 changed (communication partner)	
	2022-07-29	Introduction of term “OMS end-device”	
	2022-08-02	8.10 changed Table 38 added Table 35 changed	
	2022-08-31	3.1.4 changed Table 36 added Table 39 changed	
	2022-09-14	3.1.2.2 changed 7.2.4 changed 7.2.4.5 added 9.3.2.1 changed 9.3.7 added Table 40 changed Table 41 changed D,2, D.3 and D.4 changed	
	2022-10-08	Editorial update of tables 1.2 changed 7.2.4.7 changed	
	2022-10-15	Term “key material” replaced by “keying material” Term “master-key” replaced by “master key” Term “transport key” replaced by “communication security key Figures 16, 17, 18 changed Figures in Annex L changed Release candidate	
4.5.1	2022-11-08 to 2022-11-14	Integration of review comments Release	AG1, Achim Reissinger

Version	Date	Comment	Editor
5.0.0	2023-03-28 to 2023-10-14	Complete document: radio modes S (S1, S2) and T (T1, T2) removed 1.2 changed 2.1 revised 2.2 changed 3.1 changed 4.3 changed 4.3.2.3 added 4.3.2.5 deleted 4.3.3.2 deleted (including table 10) 7.2.4.5 note added 8.4.5.1 changed 8.7 changed 9.1 changed Figure 8 added Figure 11 updated Figure 13 changed Figure 9 deleted Table 2 changed for device types 00h, 18h, 1Ah, 1Dh, 1Eh, 1Fh and footnotes Table 41 changed Annex C removed Annex G changed: G.3 and G.7 added Annex J changed: figure revised Annex L changed: figures revised Annex Q added Annex R added Release candidate	AG1, AG1 TF Sensors, Achim Reissinger
5.0.1	2023-11-14 to 2024-02-08	Consideration of review comments Release	AG1, Achim Reissinger

Contents

Tables

Figures

1 Introduction

1.1 General

This part describes the minimum Open Metering System requirements for the wired and the wireless communication between a slave (OMS end-device) and the (stationary, usually mains powered) master (gateway or other communication unit). It covers the Physical Layer, the Link Layer, the general requirements for communication security (covered in the Authentication and Fragmentation Layer and in the Transport Layer) and the application itself. The Application Layer is focused on the M-Bus protocol. But it also supports the DLMS/COSEM protocol and an SML-based protocol. Detailed information about the required values and the time resolution are given.

This part concentrates on the requirements for OMS end-devices. This specification supports both mains powered devices (e.g. electricity meters or actuators) and battery driven devices (e.g. water meters, gas meters or thermal energy meters or sensors related to metering).

The total system overview is provided in Volume 1 [OMS-S1] of the Open Metering System specification.[1]

An overall glossary with definitions and abbreviations is provided as a separate Annex of Volume 1 [OMS-S1] of the Open Metering System Specification (general part).

The referenced standards and documents (marked with square brackets (e.g. [EN 13757-3:2018]) are listed in the Open Metering System Specification (general part).

Note that according to the use of verbal forms for the expression of provisions in standards statements with a “shall” describe mandatory requirements. Statements with a “should” describe recommendations.

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

1.2 Version History

Issue 1.0 is the very first release with limitation to unidirectional meters only.

Issue 2.0 amends regulation of the standard to access bidirectional meters or actuators. The use of repeaters was substantiated. Parts were adapted to ensure coexistence with NTA 8130.

Issue 3.0 introduces the synchronous transmission timing to support the long-term use of battery powered bidirectional repeaters. Some new CI-Fields were adopted to support the consequent use of Short and Long TPL-headers for wireless datagrams.

Issue 4.0 extends the applicable security methods. It allows compliance with the requirements of the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI) when using Annex E. It applies an update according to the release of [EN 13757-3:2013] and [EN 13757-4:2013].

Issue 4.1 is an improvement of issue 4.0. Besides a lot of minor changes, it contains an extension of Application select protocol, a new Annex K with data point descriptors, updated Annexes A and B containing encryption requirements for each data point, improved description of message counter handling, static messages, and address handling of a radio adapter.

[1] This document shall only be applied in combination with [OMS-S1] Issue 2.0.0 or higher!

Issue 4.2 is an improvement of issue 4.1. Besides many minor changes, reference updates and updated annexes it provides an updated credit counter mechanism, a detailed status byte handling and a definition of application errors. Especially for the upcoming 2-way use cases of Annex M it introduces the application layer security and it defines the applicative behaviour of an OMS end-device especially for bidirectional communications. This version introduces Annex F to support security profile C.

Issue 4.3 is an improvement of issue 4.2. It introduces two new annexes: Annex M for additional optional bidirectional use cases and Annex P for the Wired M-Bus. Consequently, Annex C was removed as the master requirements are included in Annex P. The Annexes B, E and N were revised as a result of the introduction of Annex M. Annex B contains in its revision commands. Annex E supports in its revision IDIS meters. In chapter 8.2.5 the behaviour in case of an error was revised. Further changes are listed in the document history.

Issue 4.4 integrates the communication of sensors related to metering and their device types in the new Annex C. The sensor related data points have been added to Annex B.

Issue 4.5 introduces the new term “OMS end-device”, which covers meters, sensors and actuators, introduces harmonised content index values (see 8.4.4), harmonises the message application (see 8.10), introduces a new Security profile D (see 9.3.7), applies a new concept for command action codes in Annex B, creates new use cases in Annex M and provides a correction in Annex P. Additional changes are listed in the document history.

Issue 5.0 introduces the new Annex Q defining OMS LPWAN, creates new use cases in Annex M, removes the definitions for the radio modes S and T and implements changes for the coding of sensors according to prEN 13757-3/-7:2023, thus removing Annex C. Additional changes are listed in the document history.

1.3 Reference

References to other documents are marked with square brackets. They are defined in Volume 1 [OMS-S1].

2 M-Bus Frame Structure

2.1 OMS-Layer Model

2.1.1 Overview

The M-Bus Protocol is separated in several layers based on the OSI 7 Layer Model. This document is structured according to the applied communication layers shown in Figure 1.

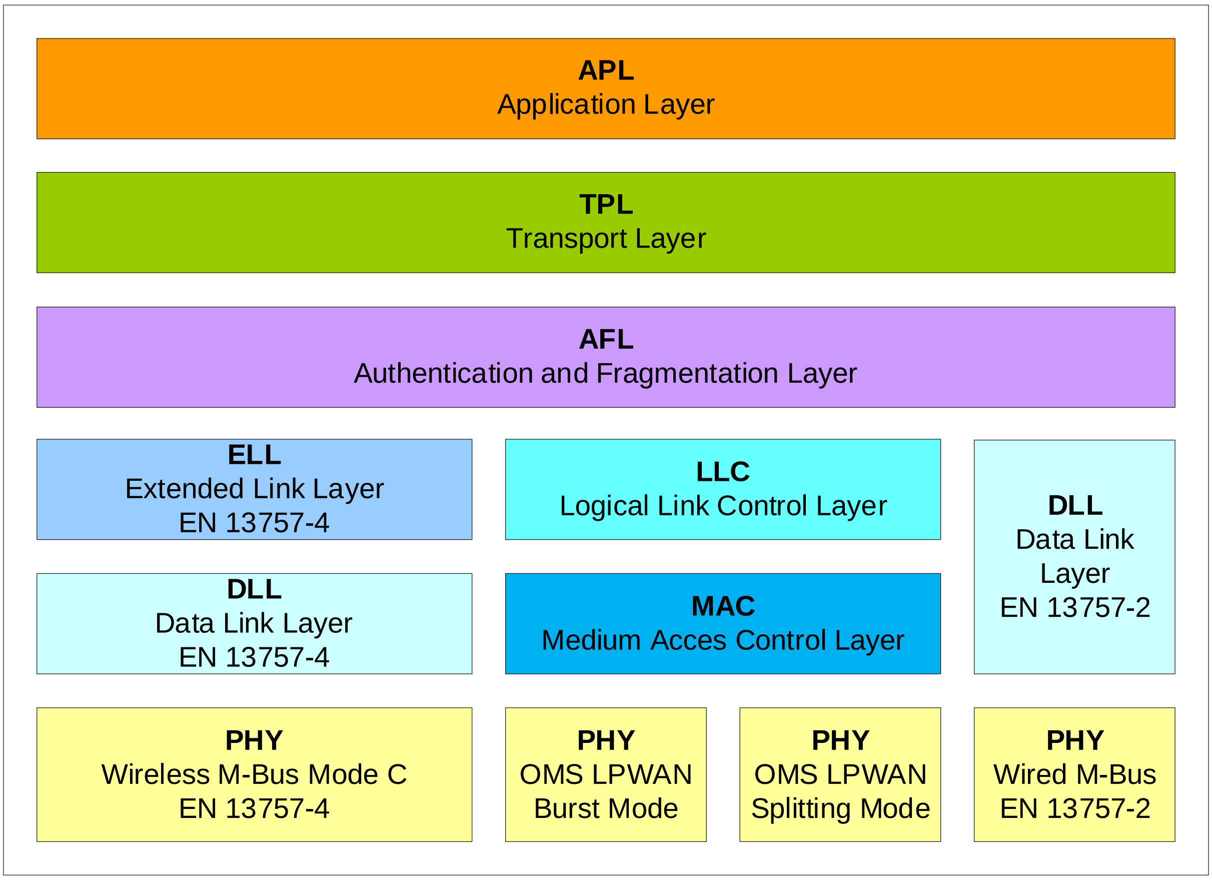


Figure 1 – OMS Layer model

The Physical Layer and the Data Link Layer are always present for Mode C and wired M-Bus.

OMS LPWAN (see Annex Q) introduces a new Link Layer containing the Medium Access Control Layer (MAC) and the Logical Link Control Layer (LLC). These layers are mandatory for OMS LPWAN with the exception of pure MAC layer frames that does not contain any higher layers. The MAC and LLC are not introduced by a CI-field.

The Transport Layer and the applied Application Layer (if existent) are always introduced by the Transport Layer's CI-Field. Optional layers[3] like ELL or AFL are introduced by special CI-Fields. In such a case the M-Bus-message contains several CI-Fields, chained to one another.

The OMS Layer Model can be realised in an OMS end-device according to one or more OMS modes from the following sub clauses.

[3] [EN 13757-5] supports an additional network layer located between ELL and AFL. This layer is never used in the Open Metering System.

2.1.2 Mode C specification

An OMS end-device according to this specification includes the layers shown in Figure 2.

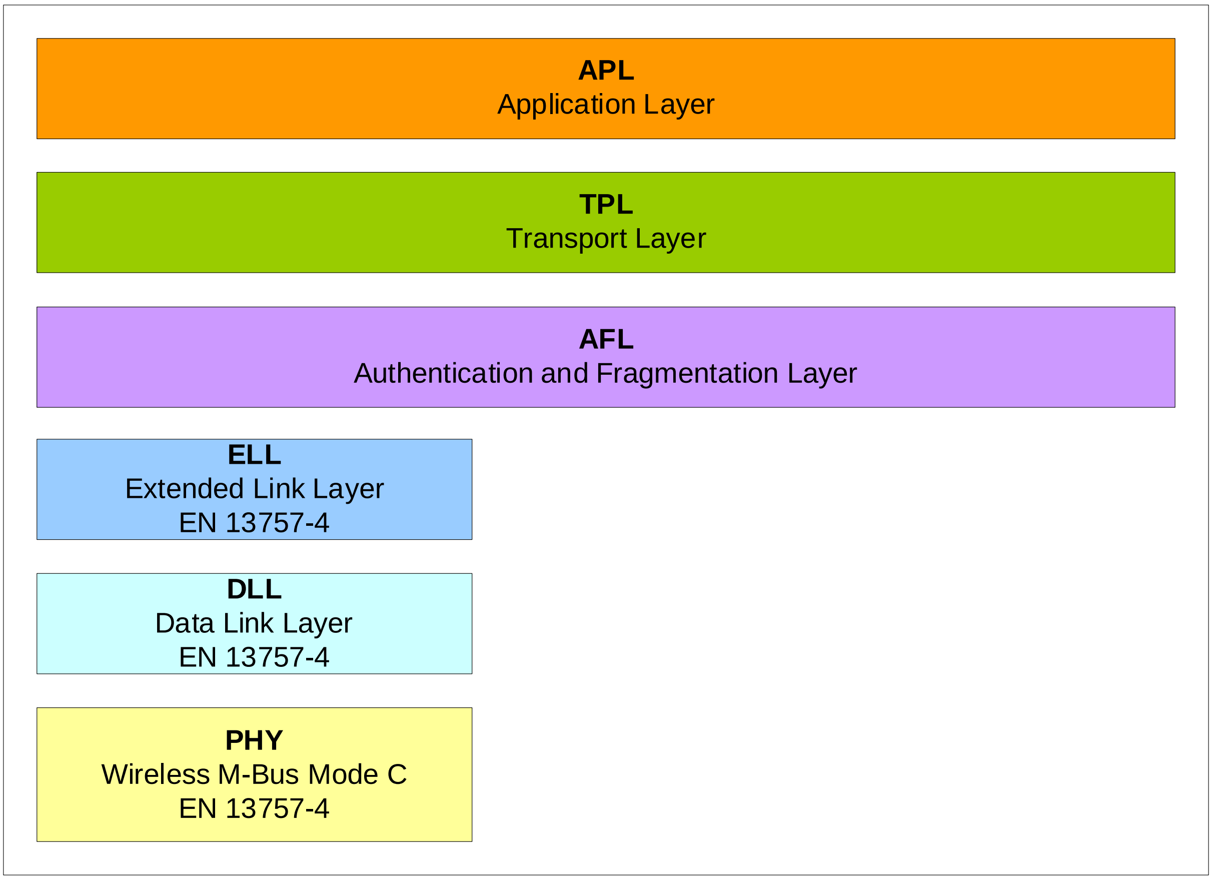


Figure 2 – Layers included in the “OMS Mode C” specification.

The PHY, DLL and ELL shall be according to [EN 13757-4].

Further requirements for this implementation are defined in this specification.

2.1.3 “OMS LPWAN – Burst Mode” specification

An OMS end-device according to this specification includes the layers shown in Figure 3.

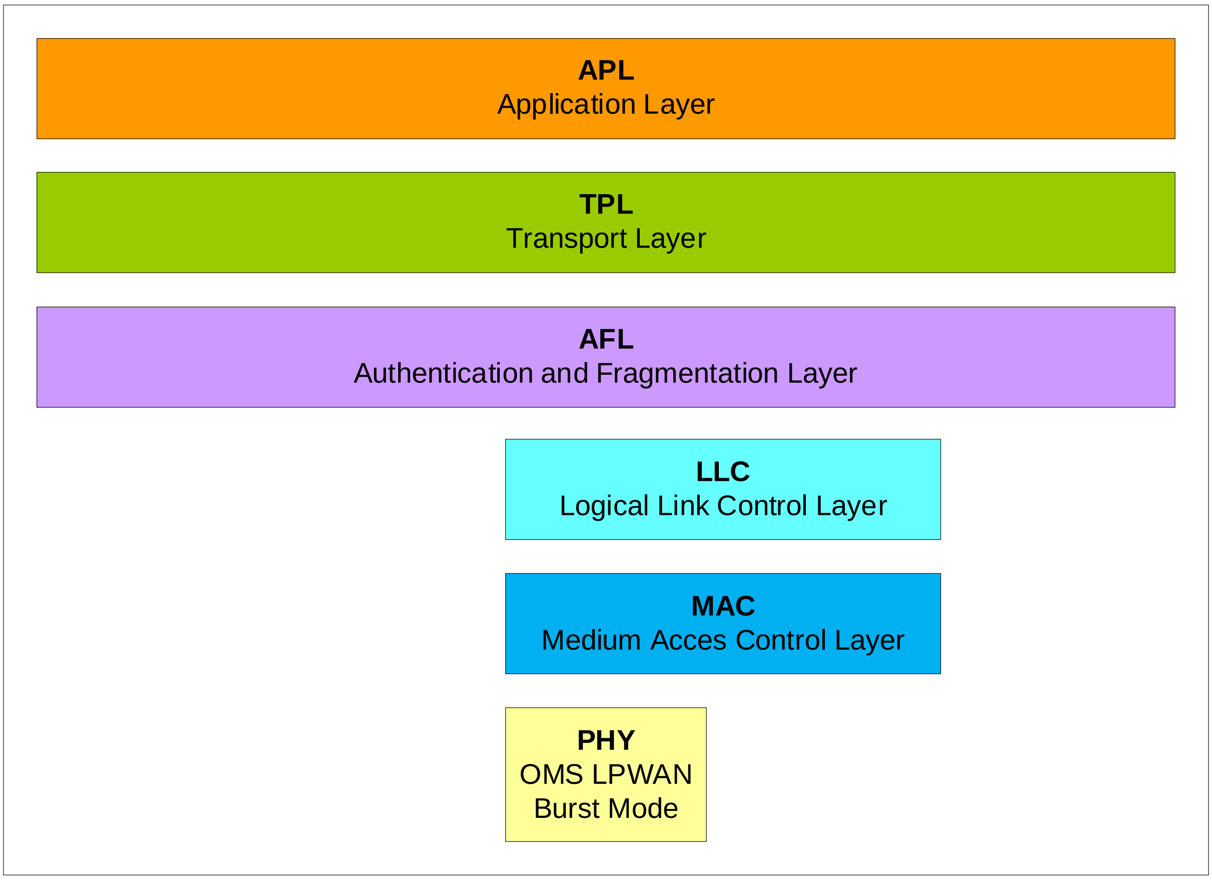


Figure 3 – Layers included in the “OMS LPWAN – Burst Mode” specification.

The PHY, MAC and LLC shall be according to Annex Q.

Further requirements for this implementation are defined in this specification.

2.1.4 “OMS LPWAN – Splitting Mode” specification

An OMS end-device according to this specification includes the layers shown in Figure 4.

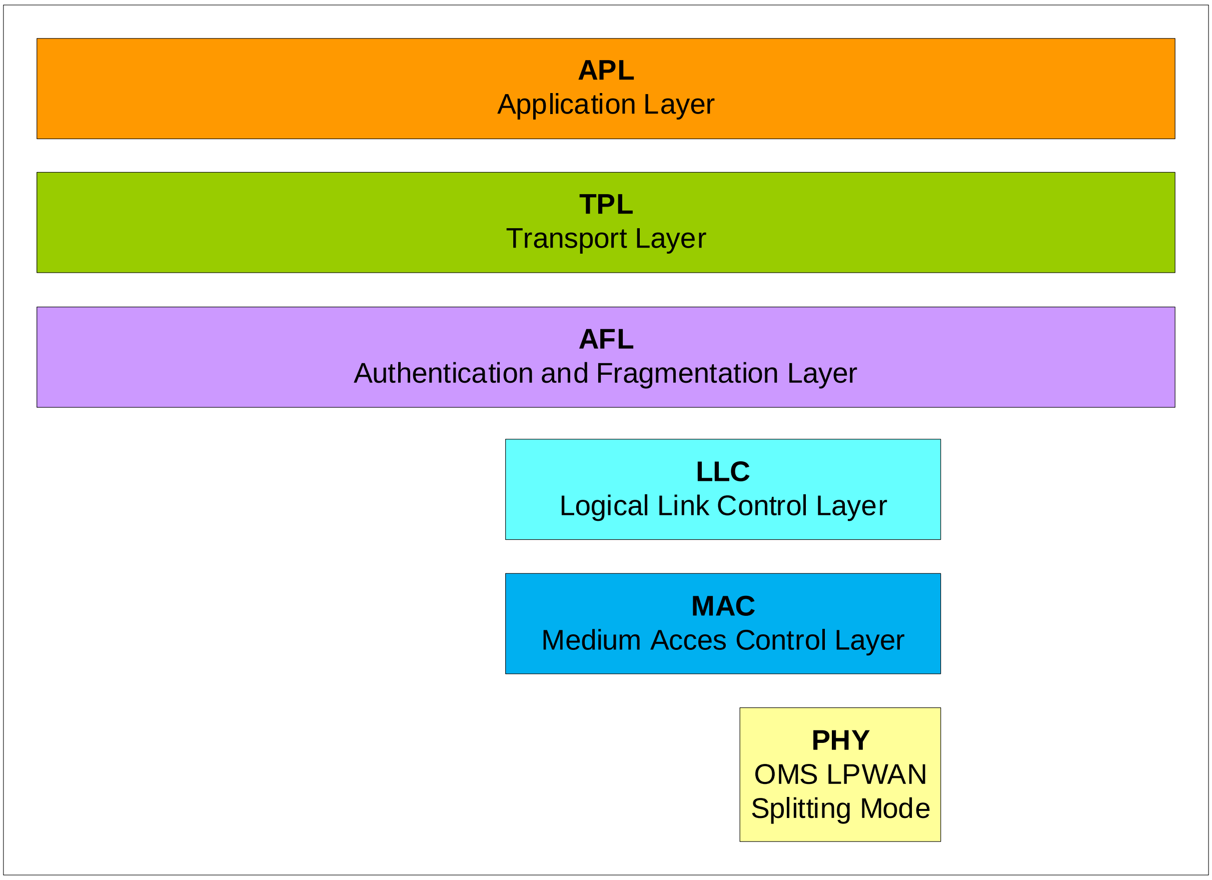


Figure 4 – Layers included in the “OMS LPWAN – Splitting Mode” specification.

The PHY, MAC and LLC shall be according to Annex Q.

Further requirements for this implementation are defined in this specification.

2.1.5 Wired M-Bus specification

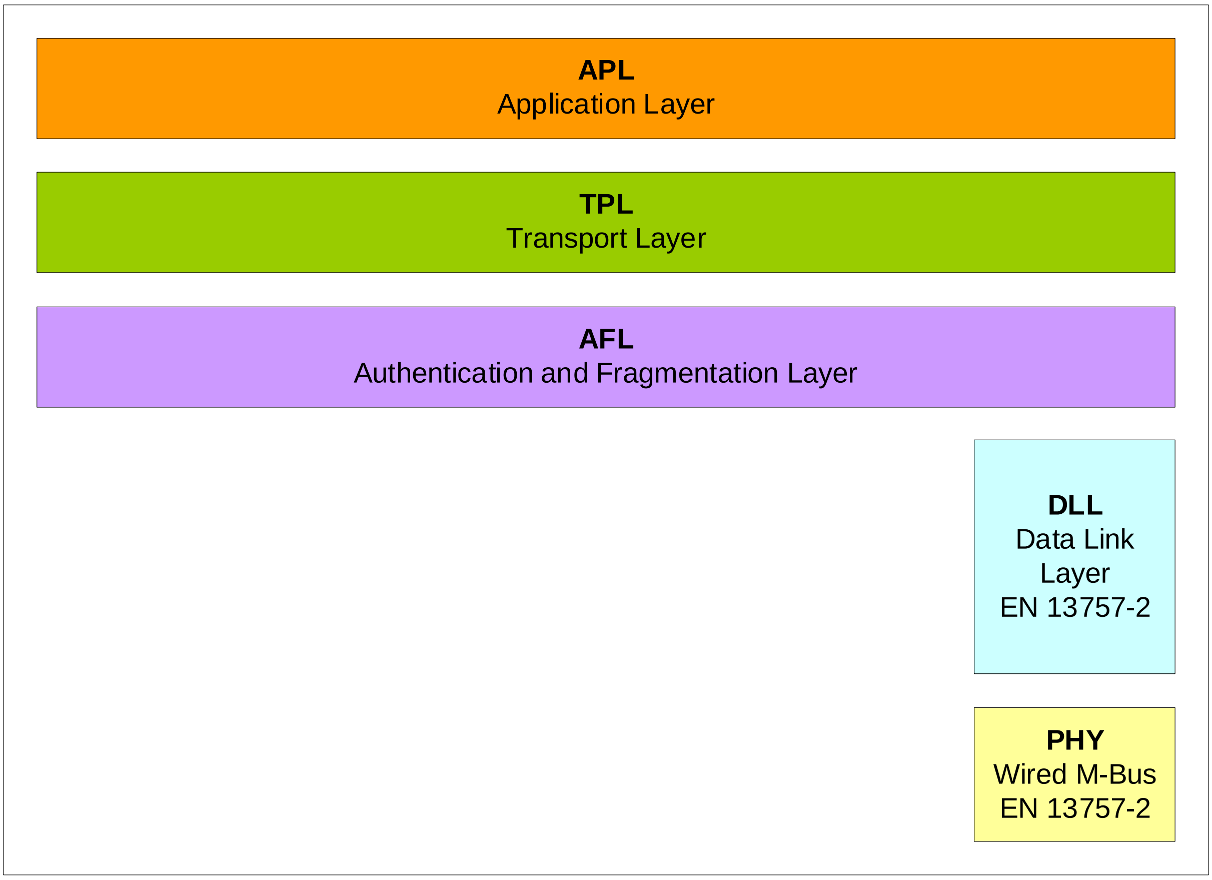


Figure 5 – Layers included in the wired M-Bus specification.

The requirements for the implementation of wired M-Bus are defined in this specification and especially in Annex P.

2.2 Supported CI-Fields

The CI-Field declares the communication layer, the transport direction (not applicable for lower layers like ELL and AFL), and the Application Protocol (if existent). The CI-Field also declares the applied type of Transport Layer header ("None", "Short" or "Long", see [EN 13757-7:2018], 7.2 to 7.5 for details).

Downlink messages are received by the OMS end-device and uplink messages are transmitted by the OMS end-device.

The following CI-Fields are allowed for OMS-Communication:

Table 1 – List of supported CI-Fields

CI-Field	Function/Layer	Up- or Down-link	TPL-header-Type	Protocol or Service
50h [d, f]	Application Reset or Select	Down	None	Application Select
51h [d, f]	Command	Down	None	M-Bus
52h [d, f]	Selection of Device	Down	None	M-Bus

CI-Field	Function/Layer	Up- or Down-link	TPL-header-Type	Protocol or Service
53h	Application Reset or Select	Down	Long	Application Select
54h [d, f]	Request of selected application	Down	None	Application Select
55h	Request of selected application	Down	Long	Application Select
56h [d, e]	Request of selected application	Down	Short	Application Select
57h [d, e]	Application Reset or Select	Down	Short	Application Select
5Ah [d, e]	Command	Down	Short	M-Bus
5Bh	Command	Down	Long	M-Bus
5Fh	Command	Down	Long	Security Management (TLS-Handshake) (see Annex F)
60h	Command	Down	Long	DLMS [b]
61h [d, e]	Command	Down	Short	DLMS [b]
62h [d, e]	Time Sync	Down	Short	Clock Synchronisation
64h	Command	Down	Long	SML [b]
65h [d, e]	Command	Down	Short	SML [b]
66h [d]	Response of selected application	Up	None	Application Select
67h	Response of selected application	Up	Short	Application Select
68h	Response of selected application	Up	Long	Application Select
6Ch	Time Sync	Down	Long	Clock Synchronisation
6Dh	Time Sync	Down	Long	Clock Synchronisation
6Eh	Application Error	Up	Short	Application Error
6Fh	Application Error	Up	Long	Application Error
70h [d, f]	Application Error	Up	None	Application Error
71h [d, f]	Alarm	Up	None	Alarm
72h	Response	Up	Long	M-Bus
74h	Alarm	Up	Short	Alarm
75h	Alarm	Up	Long	Alarm
7Ah	Response	Up	Short	Wireless M-Bus
7Ch	Response	Up	Long	DLMS [b]
7Dh	Response	Up	Short	DLMS [b]
7Eh	Response	Up	Long	SML [b]
7Fh	Response	Up	Short	SML [b]
80h	Pure Transport Layer	Down	Long	None
82h [e]	Network management	Down	Long	Network management Protocol (see [EN 13757-4:2019] clause 14)

CI-Field	Function/Layer	Up- or Down-link	TPL-header-Type	Protocol or Service
87h [e]	Network management	Up	Long	Network management Protocol (see [EN 13757-4:2019] clause 14)
88h [e]	Network management	Up	Short	Network management Protocol (see [EN 13757-4:2019] clause 14)
8Ah	Pure Transport Layer	Up	Short	None
8Bh	Pure Transport Layer	Up	Long	None
8Ch [c, e]	Extended Link Layer	Up/Down	N/A	Lower Layer Service (2 Byte)
8Eh [c, e]	Extended Link Layer	Up/Down	N/A	Lower Layer Service (10 Byte)
90h [c]	Authentication and Fragmentation Layer	Up/Down	N/A	Lower Layer Service
92h [d, e]	Network management	Down	Short	Network management Protocol (see [EN 13757-4:2019] clause 14)
93h [d, e]	Pure Transport Layer	Down	Short	None
9Eh	Response	Up	Short	Security Management (TLS-Handshake) (see Annex F)
9Fh	Response	Up	Long	Security Management (TLS-Handshake) (see Annex F)
B8h [d, f]	Set baud rate to 300 baud	Down	None	Link Layer Control
BBh [d, f]	Set baud rate to 2400 baud	Down	None	Link Layer Control
BDh [d, f]	Set baud rate to 9600 baud	Down	None	Link Layer Control
BEh [d, f]	Set baud rate to 19200 baud	Down	None	Link Layer Control
BFh [d, f]	Set baud rate to 38400 baud	Down	None	Link Layer Control
C0h	Command	Down	Long	Image transfer (see Annex M.2)
C1h	Response	Up	Short	Image transfer (see Annex M.2)
C2h	Response	Up	Long	Image transfer (see Annex M.2)
C3h	Command	Down	Long	Security Information Transport
C4h	Response	Up	Short	Security Information Transport
C5h	Response	Up	Long	Security Information Transport
C6h [d, e]	Command	Down	Short	Security Information Transport
C7h [d, e]	Command	Down	Short	Image transfer (see Annex M.2)
CFh [c, d, e, f]	M-Bus Adaptation Layer	Up/Down	N/A	MBAL acc. to prEN13757-8

[a] Footnote is obsolete and has been deleted.
[b] Refer also [EN 13757-1:2014], [EN 62056-6-1:2013], [DLMS UA] or [SML-spec]
[c] These CI-Fields are used for lower layers and may be used in combination with another CI-Field
[d] These CI-Fields shall not be used for wireless M-Bus Mode C.
[e] These CI-Fields shall not be used for wired M-Bus.
[f] These CI-Fields shall not be used with OMS LPWAN.
N/A Not applicable

2.3 Supported Device Types

This specification covers only devices with a Device Type listed in Table 2 or Table 3.

NOTE: The Device Types listed in Table 4 may also be integrated in the Open Metering System, but cannot be approved by the OMS-Compliance Test. Therefore, interoperability for these Devices Types is not guaranteed.

OMS-Gateways shall accept all the Device Types listed in Table 2 and Table 3 (except device types 25h, 31h and 36h). Optionally they may also support Device types listed in Table 4.

For further details on Device Types refer to [EN 13757-7:2018], 7.5.4, Table 13 – Device type identification.

Columns labelled “category” list the mapping from Device Type to corresponding OBIS-category / energy type as specified in subclause 3.2 of [DIN 43863-5:2012] (“Identification number for measuring devices applying for all manufacturers”).

Table 2 – Device Types of OMS end-device (certifiable with OMS-CT)

Device Type	Code	Category
Other	00h	F
Electricity meter	02h	1
Gas meter	03h	7
Heat meter	04h	6
Warm water meter (30°C ... 90°C)	06h	9
Water meter	07h	8
Heat Cost Allocator	08h	4
Cooling meter (Volume measured at return temperature: outlet)	0Ah	5
Cooling meter (Volume measured at flow temperature: inlet)	0Bh	5
Heat meter (Volume measured at flow temperature: inlet)	0Ch	6
Combined Heat / Cooling meter	0Dh	6
Hot water meter (≥ 90°C)	15h	9
Cold water meter [a]	16h	8
Pressure device [c]	18h	F
Smoke alarm device [d]	1Ah	F
Carbon monoxide alarm device [d]	1Dh	F
Heat alarm device [d]	1Eh	F
Sensor device [e]	1Fh	F
Waste water meter	28h	F
Breaker (electricity) [b]	20h	F
Valve (gas or water) [b]	21h	F

[a] Device Type 16h is to be used for cold drinking water that temporarily has been cooled or heated in order to achieve the wanted temperature (chilling/antifreeze).
[b] Annex M, OMS-UC-03 shall be applied for OMS conformance test.
[c] This device type shall support static datagrams (see 4.3.2.5) with data points acc. to Annex B.
[d] Transmitted data is used for maintenance of the device, not for the alarm itself.
[e] Shall be used only in combination with the sub device type ID11!

Table 3 – Device Types of other OMS end-devices (prepared for OMS-CT)

Device Type	Code	Category
Customer unit (display device)	25h	E
Communication controller	31h	E
Unidirectional repeater	32h	E
Bidirectional repeater	33h	E
Radio converter (system side)	36h	E
Radio converter (meter side)	37h	E
Wired adapter	38h	E

Table 4 – Device Types of not certifiable device

Device Type	Code	Category
Oil meter	01h	F
Steam meter	05h	F
Compressed air	09h	F
Bus / System component	0Eh	E
Unknown Device Type	0Fh	F
Irrigation water meter	10h	-
Water data logger	11h	
Gas data logger	12h	
Gas converter	13h	
Calorific value	14h	F
Dual register (hot/cold) water meter	17h	9
A/D Converter	19h	F
Room sensor (e.g. temperature or humidity)	1Bh	F
Gas detector	1Ch [a]	F
Reserved for switching devices	22h to 24h	-
Reserved for customer units	26h to 27h	-
Garbage	29h	F
Reserved for Carbon dioxide	2Ah	F
Reserved for environmental meter	2Bh to 2Fh	-
Reserved for system devices	30h 34h to 35h 39h to 3Fh	E
Reserved	40h to FEh	-
Not applicable (reserved for wildcard search; refer to [prEN 13757-7:2023], 7.5.4)	FFh	-
[a] Deprecated according to [prEN13757-7:2023]		

3 Address Handling

3.1 M-Bus Address

3.1.1 Overview

The M-Bus defines several types of addressing. They differ between wired M-Bus (see 3.1.2), wireless M-Bus with link layer frame format A (FFA, see 3.1.3) and wireless M-Bus with link layer frame format C (FFC, see 3.1.4).

The addresses can be handled in different layers, these are:

- the Data Link Layer (DLL)
- the Extended Link Layer (ELL)
- the Logical Link Control Layer (LLC)
- the Transport Layer (TPL).

The format of the address Field (A-Field) is different in each of those layers. The addresses used in the lower layers (DLL, ELL and LLC) are needed for communication purpose whereas the address in the TPL is used for identification of the (metering) application.

3.1.2 Wired M-Bus

3.1.2.1 Primary Address

The A-Field of the wired M-Bus uses a single byte in the DLL, which always contains the address of the slave (OMS end-device). The address of the master (gateway) is never used because only one master is allowed on the wired M-Bus. This Link Layer Address is called Primary Address (PA). The unconfigured Primary Address shall be 0. A valid address in the range from 1 to 250 has to be assigned during the configuration process if primary addressing is to be used. The addresses from 251 to 255 are used for special purposes and shall be supported in accordance with [EN 13757-2:2018].

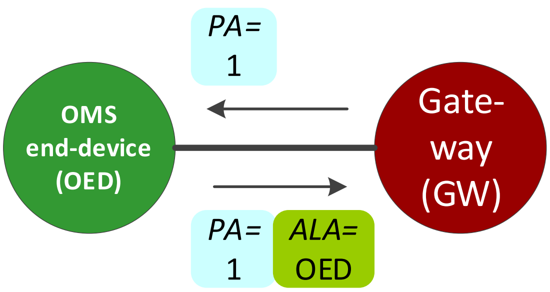


Figure 6 – Primary Address for wired M-Bus (Example)

The slave (OMS end-device) shall always respond with its own Primary Address even in the case it is addressed from the master (gateway) by Secondary Address or addressed by broadcast address.

3.1.2.2 Secondary Address

The Secondary Address is an enhancement of the limited address space of the Primary Address. It defines the Application Layer Address (ALA) and shall be worldwide unique for all types of OMS end-devices. Therefore, it shall be assigned by the OMS end-device manufacturer and shall not be changeable by any other party (e.g. MSO).

This rule is not applicable for adapters (e.g. pulse adapters, encoder adapters or protocol converters). If an adapter is used to connect an OMS end-device with the M-Bus, the adapter should transmit the OMS end-device address. For this purpose, the serial number of the OMS end-device replaces the Identification Number (part of the ALA) of the M-Bus-adapter. In this case the unchangeable Identification Number of the adapter shall additionally be transmitted in case of M-Bus application protocol with the data point “Fabrication Number" (ID1!) to avoid unsolvable address collisions.

The structure of the Secondary Address is described in subclause 3.1.5. The usage of the Secondary Address is indicated by a Primary Address 253.

The selection of an OMS end-device by Secondary Address (refer to [EN 13757-7:2018], 8.4) and the wildcard search (refer to [EN 13757-7:2018], 8.6.3) shall be supported.

An adapter should support the enhanced selection with Fabrication Number (refer to [EN 13757-7:2018], 8.5).

OMS end-devices that do not support the enhanced selection shall ignore the enhanced selection command of the master (gateway).

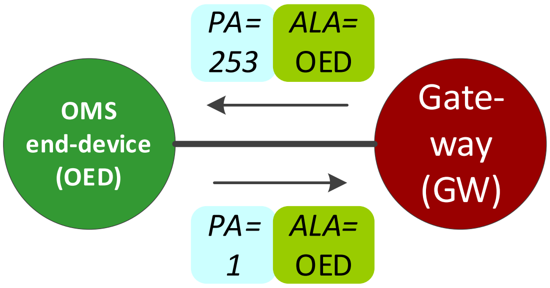


Figure 7 – Secondary Addresses for wired M-Bus (Example)

The ALA of the OMS end-device shall always be in each M-Bus-message of the slave (OMS end-device). The master (gateway) shall apply the ALA of the OMS end-device at least in case of encryption or during the selection (refer to [EN 13757-7:2018]) of the slave (Figure 7).

NOTE 1: The address field of the ALA exists only if a Transport Layer with Long TPL-header is used (see 2.2 and Annex D).

NOTE 2: When a valid Primary Address is applied or the slave (OMS end-device) is clearly selected, then the (unencrypted) message of the master (gateway) may not contain a Secondary Address (ALA) (Figure 6).

If an adapter uses encrypted data transfer, then its Fabrication Number shall be transmitted in the unencrypted area.

3.1.3 Wireless M-Bus (Frame Format A)

3.1.3.1 General

The frame format A shall be used in case of the wireless M-Bus Mode C.

3.1.3.2 Link Layer Address (LLA)

The address field of the Data Link Layer always contains the address of the sender. This can be the address of the OMS end-device/repeater/gateway (in case of an integrated radio interface) or the address of the RF-Adapter (which connects the hosted device to the radio channel). Its structure is described in subclause 3.1.5. The Link Layer Address shall be used in each wireless M-Bus-datagram.

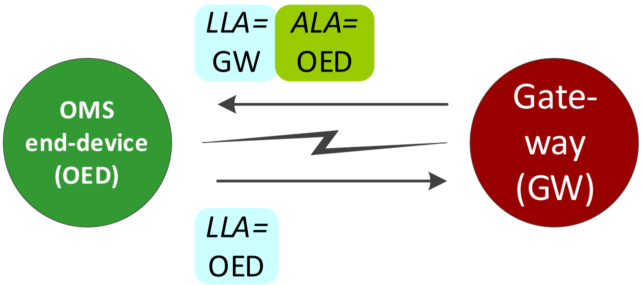


Figure 8 – Addresses for wireless M-Bus (without ELLA)

The Link Layer Address shall be unique worldwide for all wireless M-Bus OMS end-devices. Therefore, it shall be assigned by the manufacturer and shall not be changeable by any other party (e.g. MSO). The assignment of an additional address (if necessary, e.g. when using an external RF-Adapter) has to be applied in the Transport Layer using an Application Layer Address (see 3.1.3.4).

3.1.3.3 Extended Link Layer Address (ELLA)

The address field of the Extended Link Layer always contains the destination address (OMS end-device/adapter/gateway). It is only used for wireless M-Bus. Its structure is described in subclause 3.1.5.

The ELLA only exists if a long Extended Link Layer is applied (see 5.2.2.2).

A received datagram with an ELLA not matching to its own Link Layer Address shall be ignored, even if the ALA is correct.

The Extended Link Layer Address is only required in the following cases.

1. Addressing of a not allocated communication partner

To avoid conflicts in bidirectional radio communication it is essential that an OMS end-device is allocated to only one dedicated gateway. This allocated gateway should not use the ELLA to contact the OMS end-device (except when case 2, 3 or 4 is applicable). Any other device (such as a service tool) shall always transmit the ELLA to identify itself as a non-allocated communication partner on the OMS end-device and compare the received ELLA with its own address. An OMS end-device response (RSP-UD, ACK, NACK) without ELLA shall only be accepted by the allocated gateway.

2. Response to a request with ELLA

If a device receives a datagram with an ELLA (identical to its own Link Layer Address), it shall respond with an ELLA (holding the Link Layer Address of the other device). If the received ELLA does not fit to its own Link Layer Address, the datagram shall be ignored.

3. Fragmented Messages

If a message is fragmented (by using the AFL - see clause 6), each fragment (datagram) shall apply the ELLA. This is required because the Application Layer Address (ALA) will only be present in the first fragment. Even the request (REQ-UD2) and the acknowledge (ACK) of the concerning fragment shall apply the ELLA of the communication partner (also see Annex L).

NOTE: The first REQ-UD2 of a fragmented message may contain no ELLA (but always an ALA). The first RSP-UD as well as all following fragments of this message require the ELLA.

4. Message to an RF-Adapter

If a gateway responds to an OMS end-device using an RF-Adapter, the gateway shall apply the ELLA in the datagram (see Figure 10).

Message types SND-NR, SND-IR, ACC-NR, and ACC-DMD should not apply the ELLA.

Figure 9 and Figure 10 show the usage of the ELLA beside the other address fields.

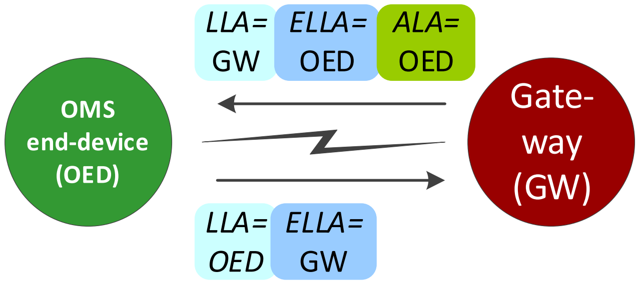


Figure 9 – Addresses for wireless M-Bus (with ELLA)

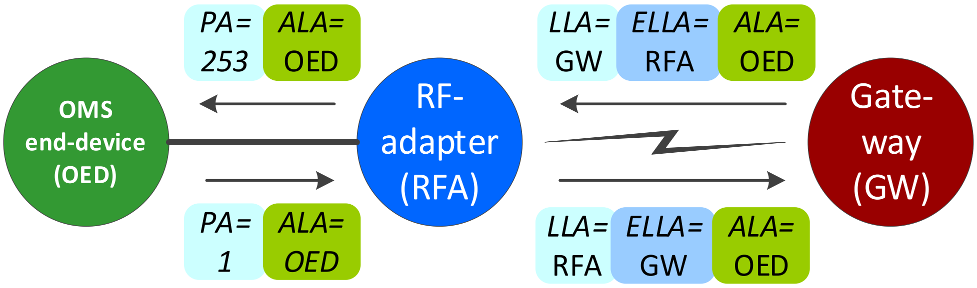


Figure 10 – Addresses for wired and wireless M-Bus (with ELLA, example)

3.1.3.4 Application Layer Address (ALA)

The address field of the Transport Layer always contains the address of the application (OMS end-device). Its structure is described in subclause 3.1.5.

The Application Layer Address shall always be present in downlink messages (to the OMS end-device) and in uplink messages (from the OMS end-device), if an external RF-Adapter (Device Type 37h) is used. For OMS end-devices with an integrated radio module the Link Layer Address acts as Application Layer Address as well (see Figure 8).

A received datagram with a not matching ALA (if existent) shall be ignored by the OMS end-device, even if the ELLA is correct.

NOTE 1: The RF-Adapter can also be addressed directly using the ALA with the RF-Adapter address.

NOTE 2: The address of the communication partner of the OMS end-device (like gateway, repeater or service tool) is never applied in this address field.

NOTE 3: The address field of the ALA only exists, if a Transport Layer with Long TPL-header is used (see 2.2 and Annex D).

NOTE 4: The additional usage of an ALA is also allowed (but not requested), when LLA and ALA are identical.

The detection of the ALA shall be processed according to the algorithm in Figure 11.

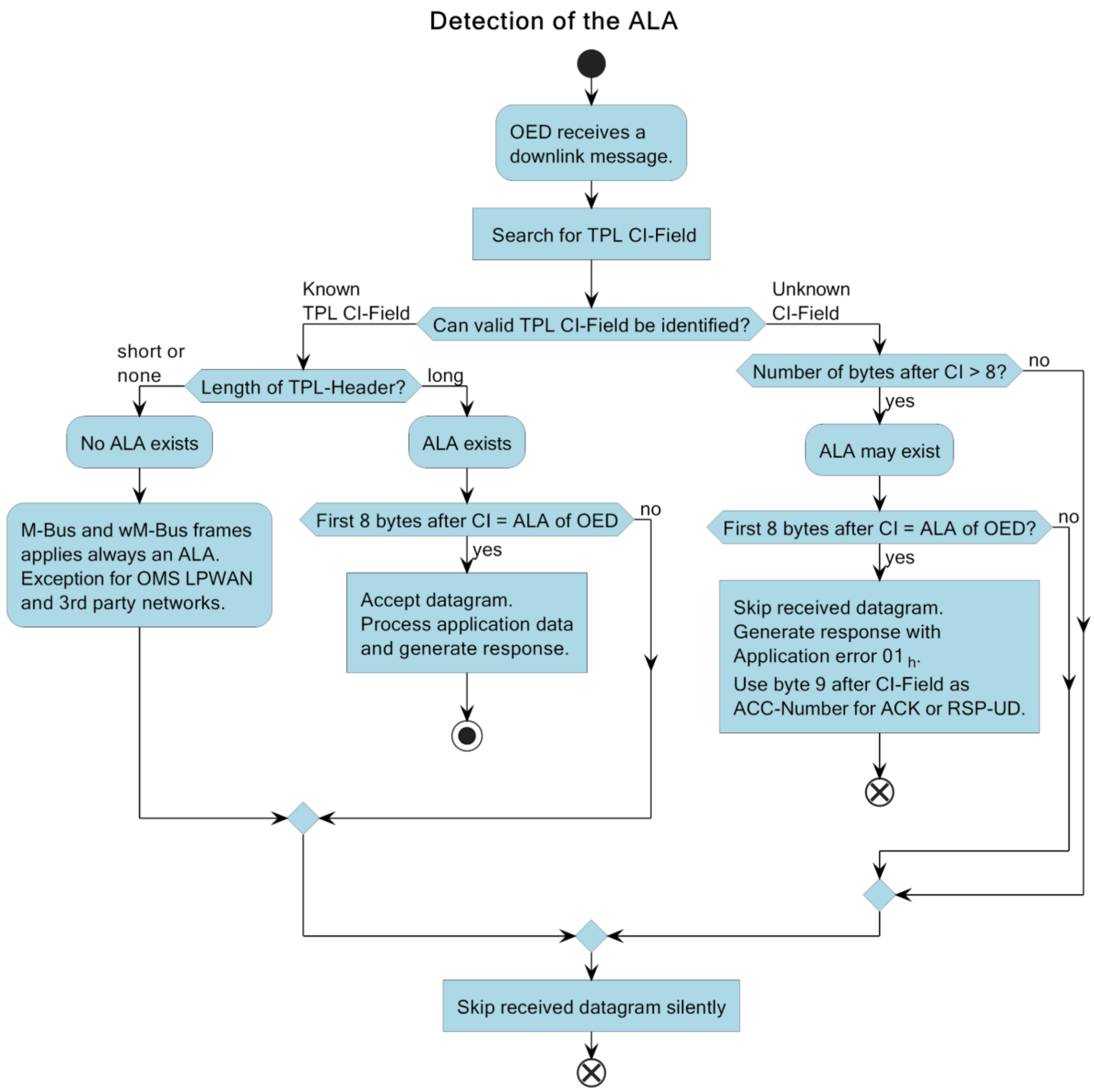


Figure 11 – Detection of the ALA

3.1.4 Wireless M-Bus (Frame Format C)

3.1.4.1 General

The frame format C in the LLC layer shall be used together with the M-Bus MAC layer in case of OMS LPWAN (see Annex Q). It has a flexible design and can contain both, the transmitter address (TXA) and the receiver address (RXA). This makes the use of the ELL (as described in 3.1.3.3) obsolete. The application address (ALA) in the TPL is only needed in case an external RF-Adapter (Device Type 37_h) is used.

The TXA is a functional replacement of the LLA. The RXA is a functional replacement of the ELLA. The flexible structure of the frame format C (FFC) allows to apply them only if needed with help of the controlling bits in the LC[0]-field (see Annex Q, Q.4.2.2 LC-Field).

Figure 12, Figure 13 and Figure 14 provides an overview of different address usage with FFC.

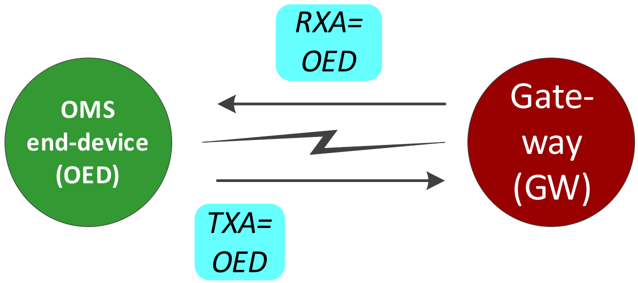


Figure 12 – Address usage in FFC for an allocated gateway

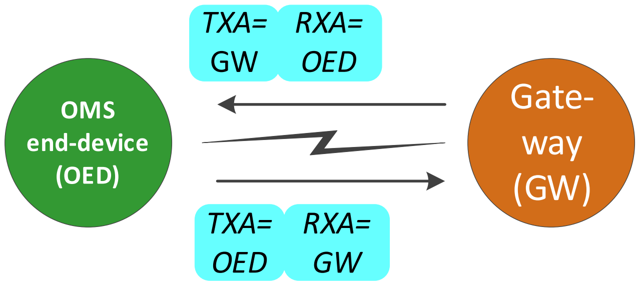


Figure 13 – Address usage in FFC for a not allocated gateway

NOTE: An allocated gateway may also send the TXA-field with its own address if it sets the RRX bit (see Annex Q, Q.4.2.2 LC-Field) in downlink.

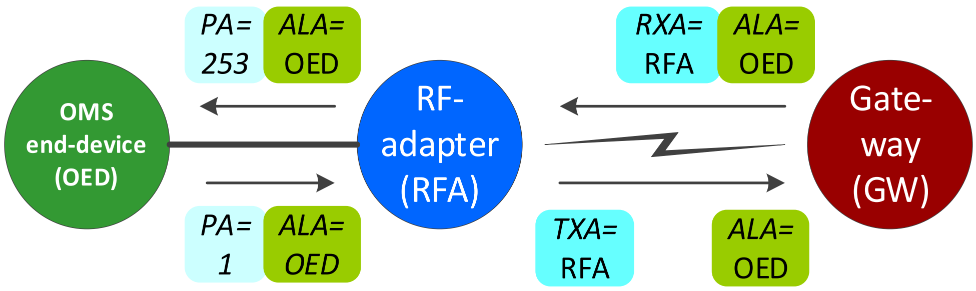


Figure 14 – Address usage in FFC with RF-Adapter

3.1.4.2 Transmitter Address (TXA)

The transmitter address is contained in the LLC layer within the M-Field and the A-Field if indicated by the “Transmitter Address Present” (TAP) bit in the LC[0]-field. Its structure is described in subclause 3.1.5. In uplink direction it contains the address of the sender that is either the OMS end-device or the RF-Adapter. In downlink direction it contains the sender address, i.e., the address of the gateway or the communication partner.

The TXA is not mandatory in all datagrams. It can be avoided in the following cases:

1. Uplink MAC frame types without LLC (see Annex Q, Table Q.74 MAC Frame types)
2. Downlink frames from an allocated gateway

The TXA (like the LLA, see 3.1.3.1) shall be worldwide unique for all wireless M-Bus OMS end-devices, RF-Adapters and gateways. Therefore, it shall be assigned by the manufacturer and shall not be changeable by any other party (e.g. MSO).

3.1.4.3 Receiver Address (RXA)

The receiver address is contained in the LLC layer within the M2-Field and the A2-Field if indicated by the “Receiver Address Present” (RAP) bit in the LC[0]-field. Its structure is described in subclause 3.1.5. It contains the destination address in uplink (e.g. the gateway) and downlink (the address of the OMS end-device or the RF-Adapter) direction.

The RXA is not mandatory in all datagrams. It can be avoided in the following cases:

1. Uplink MAC frame types without LLC (see Annex Q, Table Q.74 MAC Frame types)
2. Unsolicited uplink frames
3. Uplink frames inside a “downlink communication session” (see Annex Q, Q.3.3.5) where the communication partner did not request the uplink receiver address with the RRX bit of the LC[0]-field (see Annex Q, Q.4.2.2 LC-Field).

3.1.4.4 Application Layer Address (ALA)

The ALA is the address field in the TPL. Its structure is described in subclause 3.1.5.

The address of the OMS end-device is located in different address fields depending on the uplink or downlink and the usage of an internal/integrated or external radio module. Table 5 depicts the location of the OMS end-device address for the different cases.

Table 5 – Location of the OMS end-device address

Direction	Uplink	Downlink
Integrated radio	TXA	RXA
External RF-Adapter	ALA	ALA

A received datagram including a not matching ALA shall be ignored by the OMS end-device.

NOTE 1: The RF-Adapter can also be addressed directly using the ALA with the RF-Adapter address.

NOTE 2: The address field of the ALA only exists if a Transport Layer with Long TPL-header is used (see 2.2 and Annex D).

3.1.5 M-Bus Address Elements

The LLA, the ELLA, the TXA and the RXA for wireless M-Bus as well as the ALA for both wired and wireless M-Bus always consist of these four parts:

- Identification Number (Device ID)
- Manufacturer ID
- Version
- Device Type

Usage of these elements shall be in accordance with [EN 13757-7:2018], 7.5.1 to 7.5.4.

The registered FLAG ID from the DLMS UA shall be used as the Manufacturer ID (https://www.dlms.com/flag-id/).

The Version field is not restricted in use for naming the software version. It may apply also for other address purposes like coding of the manufacturer's location as long as it grants a worldwide unique addressing of this OMS end-device. Additional OMS end-device identification schemes like customer number or OMS end-device location may be implemented via corresponding data records within the Application Layer.

See 2.3 for the limitation of the Device Type.

The order of the address elements differs between the lower layer addresses (LLA, ELLA, TXA, RXA) and the ALA.

The ALA shall apply to the structure as given in [EN 13757-7:2018], 7.4.

The lower layer addresses shall apply to the structure as given in [EN 13757-7:2018], 8.3.

Address examples can be found in Annex A of [CEN/TR 17167:2018] and Annex N of this specification.

3.2 DIN Address

[DIN 43863-5:2012] defines a common structure Meter-ID. This DIN Address structure is the base for meter management.

The structure of the DIN Address is shown in Table 6.

Table 6 – Structure of the DIN Address

Digit	14	13	12	11	10	09	08	07	06	05	04	03	02	01
Meaning	OBIS -cat.[4]	Manufacturer ID			Fabrication Block		DIN-Fabrication Number							
Example	7	Q	D	S	0	1	1	1	2	2	3	3	4	4

The DIN Address may be used on the label of a metering device. For the Link or Transport Layer of the wired or wireless M-Bus only the M-Bus addresses are allowed. However, there is a clear relation between the ALA and the DIN Address and one address type can be converted from one to another. The address conversion shall be done according to the following rules.

OBIS-cat. [4]	Energy type (e.g. electricity) based on OBIS code value group A. (Note that categories “E” and “F” are listed in DIN 43863-5:2012, but only energy type “F” for “Other media” is listed in Blue Book ed. 13 of DLMS User Association.) For conversion between the address types use Table 2, Table 3, and Table 4 in 2.3. These tables list the assigned OBIS- category / energy type for each M-Bus Device Type.
Manufacturer ID	This field corresponds to the Manufacturer ID of the M-Bus Address. Note that the Manufacturer ID of the DIN Address is presented with ASCII-letters (A-Z, upper case only), whereas the M-Bus uses a 2 byte binary code. Conversion between both is described in [EN 13757-7:2018], 7.5.2. The most significant bit of the M-Bus Manufacturer ID is pre-set to 0 (Hard address).
Fabrication Block	According to [DIN 43863-5:2012] the usage of the Fabrication Block is manufacturer specific. This is comparable with the Version Field of the M-Bus Address. For conversion between M-Bus Address and the DIN Address the Fabrication Block holds the same content as the Version Field (and vice versa).
DIN-Fabrication Number	The DIN-Fabrication Number contains the serial number of the meter. It is equal to the Identification Number of the M-Bus Address. For the conversion between address types the DIN-Fabrication Number of the DIN Address gets the same content like the Identification Number of the M-Bus Address (and vice versa).

Each M-Bus Device Type can be unambiguously converted to an OBIS-Category. Reversely, multiple Device Types are mapped to a single OBIS- category / energy type. Therefore, a conversion can only be unique, if all Device Types with the same OBIS- category / energy type differ in Identification Number, Manufacturer ID or Version. Consequently, the manufacturer shall ensure that the M-Bus Addresses of all of their meters have unique combinations of Identification Number and Version within the same OBIS- category / energy type.

[4] Corresponds to “OBIS- category / energy type”

The DIN Address may also be made available as a data point on the OMS end-device interface, as defined in 8.4.5.2.

3.3 Address Handling by Adapters

An RF-Adapter or an M-Bus-Adapter transports the address of the hosted OMS end-device. Figure 15 specifies how the adapter shall detect and convert the OMS end-device address to an M-Bus-address.
In case the adapter identifies the hosted OMS end-device by its DIN-Address, the conversion to an M-Bus Address may not be unique. Table 7 shows recommended default values for a conversion from OBIS-category to Device Type. A better applicable Device Type can however be used instead. The selected Device Type shall be linked to the given OBIS-category according to Table 2, Table 3, and Table 4.

Table 7 – Default Device Type in case of DIN-Address conversion

Category	Default M-Bus Device Type	Code
1	Electricity meter	02h
2	-	-
3	-	-
4	Heat Cost Allocator	08h
5	Cooling meter (Volume measured at return temperature: outlet)	0Ah
6	Heat meter	04h
7	Gas meter	03h
8	Water meter	07h
9	Warm water meter (30°C … 90°C)	06h
A	-	-
B	-	-
C	-	-
D	-	-
E	Bus / System device	0Eh
F	Unknown Device Type	0Fh

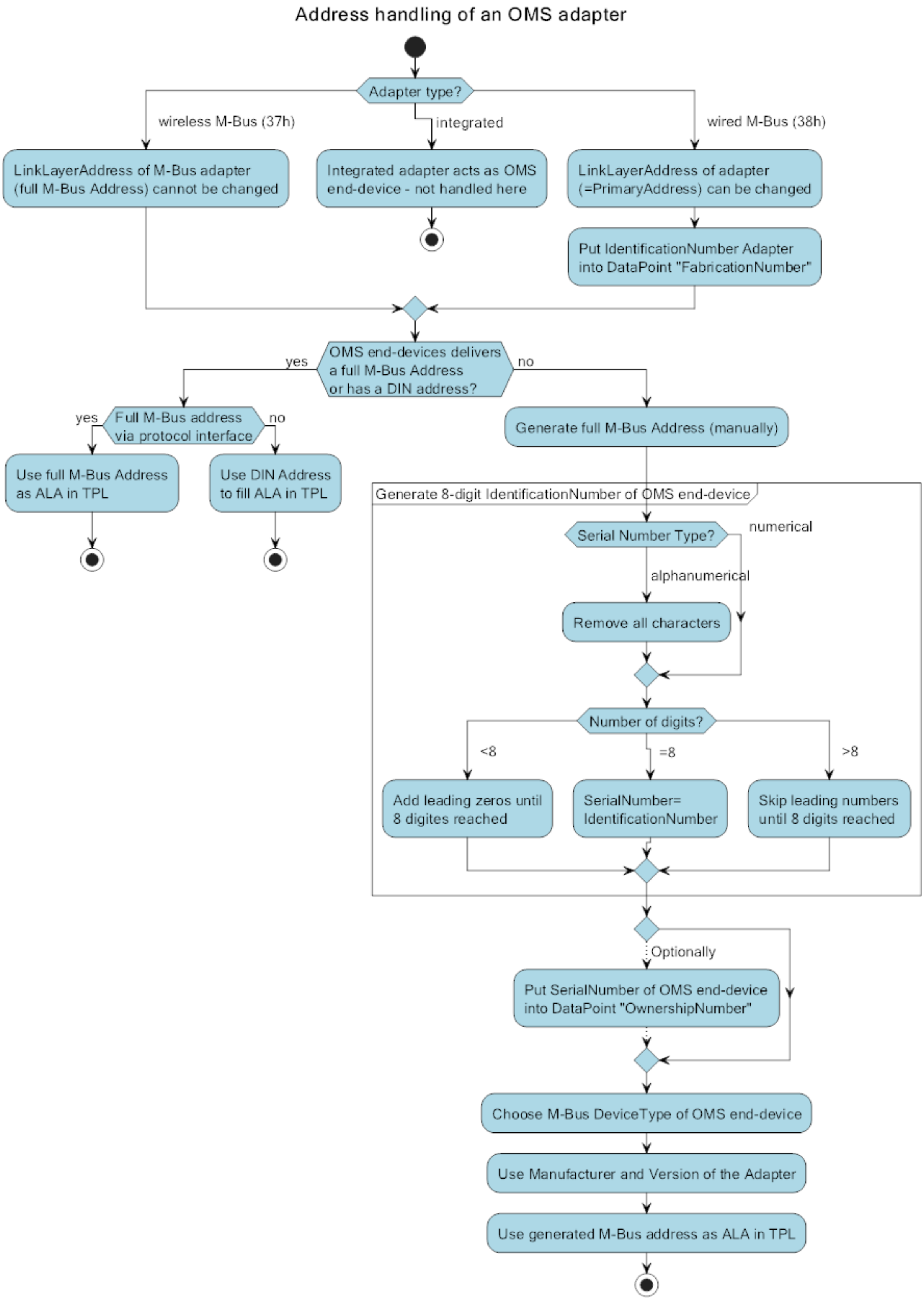


Figure 15 – Address handling of an RF or M-Bus adapter

4 Physical Layer

4.1 General

Data shall be collected from the OMS end-devices using two-wire M-Bus via pull mode, or wM-Bus (wireless M-Bus) via push mode. This means that OMS end-devices transmit metering data by radio in regular intervals or they have to be queried via wired M-Bus by the gateway. Optionally the gateway may also query metering data from bidirectional wireless M-Bus OMS end-devices.

4.2 Wired Communication (Wired M-Bus)

4.2.1 General

Normative and informative requirements for the M-Bus are defined in Annex P and [EN 13757-2:2018].

4.2.2 Electrical Specification

For wired connections the Physical Layer M-Bus according to the European Standard [EN 13757-2:2018] is used. It is a two-wire system, which optionally also provides power to the devices. The number of wired M-Bus devices that can be controlled by a gateway, shall be specified by the manufacturer. The minimum requirements are those of a Mini-Master as described in [EN 13757-2:2018].

4.2.3 Hardware Connections and Wiring

The bus interfaces of the slaves are polarity independent, which means that the two bus lines can be reversed without affecting the operation of the slaves. Besides protection aspects, this also leads to a simplified installation of the bus system. In order to maintain correct operation of the bus in case of a short circuit of one of the slaves, these shall have a serial resistor with a total nominal value of 430±10 Ω in the bus line. This limits the current in case of a short circuit to a maximum of 100 mA (42 V / 420 Ω). For the requirements for wiring and installation refer to [EN 13757-2:2018] and Annex P.

4.3 Wireless Communication (Wireless M-Bus)

4.3.1 Modes and Requirements

[EN 13757-4:2019] describes different variants for wireless metering communication. They cover many types of metering communication including mobile and stationary readout modes. The Open Metering System scenario requires a stationary receiver. This document extends [EN 13757-4:2019] to allow OMS LPWAN and optional single hop relaying for radio range extension. Multi hop relaying of these data via other (optionally battery powered) OMS end-devices is not supported by this specification.

As for the various modes described in [EN 13757-4:2019], only the modes C1 and C2 are supported by this specification. Additionally, the wireless M-Bus mode OMS-LPWAN defined in Annex Q is supported too. These modes operate in duty-cycle limited sub bands of the 868 – 870 MHz license free frequency range. The duty cycle is not a limiting factor for the Open

Metering System but limits the band occupation time for all systems operating in these frequency bands.

NOTE 1: OMS LPWAN increases the robustness against disturbers by applying FEC. This results in a higher channel occupancy.

A limitation of the total average transmission duty cycle per hour to 0,02 % is recommended for Mode C. This is required to limit the collision rate e.g. in dense situations. CEPT/ERC/REC 70-03 E, refer to [ERC 70-03], and ETSI EN 300220-1 [ETSI EN 300 220-1] describe further requirements for the Physical Layer.

NOTE 2: The OMS LPWAN duty cycle limitations are provided in Annex Q.

There are unidirectional modes like C1, UL-S1 or UL-B4 where the OMS end-device frequently (seconds to hours) transmits datagrams containing OMS end-device identification together with metered data. This unidirectional function is sufficient to support all mandatory communication for an OMS end-device within the framework of the Open Metering System.

There is also compatible bidirectional enhancement of the respective unidirectional mode. It enables an optional gateway to OMS end-device communication following an OMS end-device to gateway datagram. [EN 13757-4:2019] describes all requirements (also applicable for testing conditions) for the supported modes C1 and C2. The same applies for the OMS LPWAN sub-modes of Annex Q.

Due to required battery lifetime, most meters and some actuators cannot support a continuous receive mode. A gateway initiated (“Pull”) communication with the OMS end-device is possible. But any such a gateway to OMS end-device communication is typically limited to a time slot directly following an OMS end-device to gateway communication (except for mains powered devices). Since the OMS end-device transmits frequently, the resulting transmission delay (varying from seconds to hours) seems acceptable. An actuator shall transmit at least its unique ID and its status and wait after each transmission for a possible datagram from the gateway as described in [EN 13757-4:2019]. For a breaker, as the typical actuator, the maximum time interval between such transmissions shall be the same as the maximum time interval for meter transmissions of the same medium (i.e. electricity or others) as shown in Table 8.

For certain communication situations between the gateway and an optional actuator this might not be sufficient. Thus, actuators with faster reaction time requirements should be mains powered.

Link Control Bits in the MAC Layer, Extended Link Layer or Configuration Field of the OMS end-device datagram signal to the gateway whether the device can receive data (i.e. implements the bidirectional mode) and whether it can receive continuously or only immediately after each transmission.

The OMS end-device and gateway manufacturers decide which of the supported mode are implemented in their products. This requires clear labelling of the devices as well as the respective data sheets so that the customer has the possibility to choose between interoperable combinations. A gateway may support communication with one, several, or with all of the radio communication modes mentioned.

Countries being members of CEPT (e.g. EU, EEA and more) shall use the frequencies specified in [EN 13757-4:2019], which are based on CEPT/ERC/REC 70-03 [ERC 70-03] (except Russia). Other countries where these frequencies are not allowed shall use the alternative frequencies defined in Annex O of this document.

4.3.2 Wireless Data Transmission Intervals

4.3.2.1 Synchronous versus Asynchronous Transmission

OMS end-devices shall use the strictly synchronous transmission scheme as specified

- for Mode C in [EN 13757-4:2019], 12.6.2 and
- for OMS LPWAN in Annex Q, Q.2.4.6.4 and Q.2.5.6.3.

The synchronous transmission is signalled by the synchronous bit S. The synchronous transmission timing can be predicted using the Access number. The position of this information is located in different layers of the datagram depending on the applied wireless M-Bus mode

- Mode C: If the Extended Link Layer is present, Access Number and Synchronous Bit (see 5.2.2.2.3) in the ELL shall be used for synchronous timing. Otherwise the Access Number of the Transport Layer and the Synchronous Bit in the Configuration Field shall be applied.
- OMS LPWAN: This wireless M-Bus mode provides a Logical Link Control Layer (LLC) using Frame format C. This LLC combines elements of DLL and ELL. The Synchronous Bit and the Access number of the LLC shall be used (see Annex Q, Q.4)

As described in [EN 13757-4:2019], 12.6.2, additional asynchronous transmissions are allowed. The Access Number handling of asynchronous transmissions is specified in [EN 13757-7:2018], 7.5.5.2 and pictured in Figure 16.

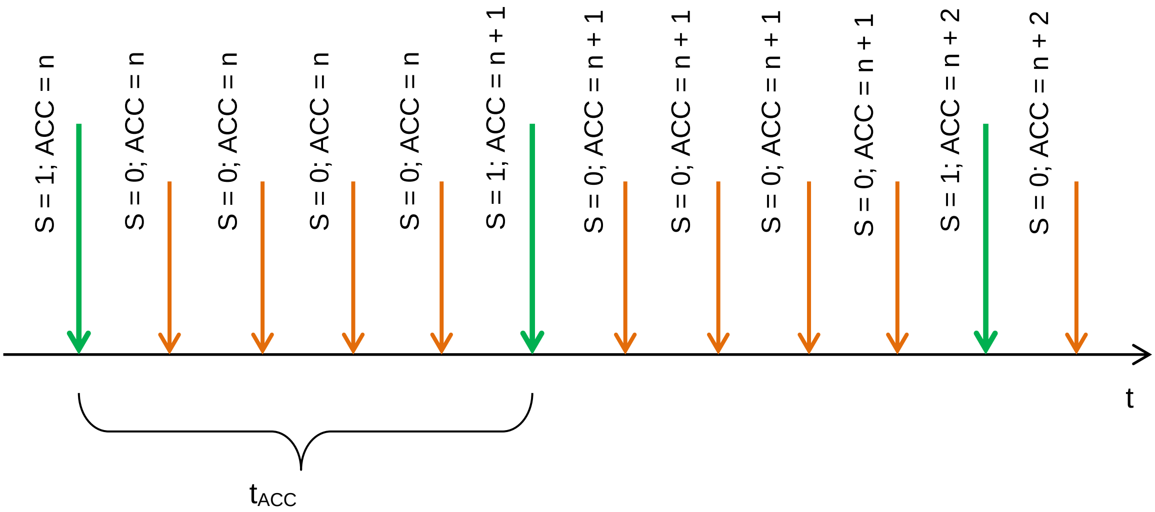


Figure 16 – Access number for synchronous and asynchronous transmissions

Legend:

S	S = 1: synchronous datagram; S = 0: asynchronous datagram
ACC	Access Number
t_{ACC}	individual transmission interval from the datagram with the Access Number ACC = n to the next synchronous transmission with ACC = n+1

The synchronous transmission shall be one of the message types SND-NR, ACC-DMD, or ACC-NR (see Table 16). If the nominal transmission interval (refer to [EN 13757-4:2019], 3.12 and 12.6.2) is smaller than the selected update interval of consumption data (see Table 8), then one or several ACC-NR may be used for synchronous transmission between the synchronous transmissions of the SND-NR. The ratio of ACC-NR versus SND-NR (respectively ACC-DMD in case of alert) shall be n to 1 to allow a reception of every n^{th} datagram only (with n = 0 … 15) by a battery operated receiver. The ratio shall not be changed after the installation of the OMS end-device.

The start of the first synchronous transmission shall be stochastic. It is not allowed to fix the synchronous transmission exactly to a common event like a special time or a power-up after a voltage breakdown. This is required to avoid a concurrent use of the radio channel by many OMS end-devices. Refer also to subclause 7.2.2.1.

Asynchronous transmissions are intended for any transmission outside the synchronous transmission time slot. OMS end-device message types RSP-UD, ACK, NACK, SND-IR shall be asynchronously transmitted. Nevertheless, message types SND-NR, ACC-DMD, or ACC-NR may be asynchronously transmitted as well (see Table 16).

A bidirectional OMS end-device should provide a reception window (after a transmitted synchronous datagram) per interval t_{NOM} (max) according to [EN 13757-4:2019], 12.6.2, Table 36 – Maximum values of nominal transmission interval. The bidirectional OMS end-device shall not provide less reception windows as defined in 4.3.4.

4.3.2.2 Interval of Consumption Data

OMS end-devices shall provide a minimum data granularity (see Table 8) of the consumption data points as required in 8.4.4 for billing purpose. This can either be done with a regular update of those data points (high data actuality, typical for Mode C) or by providing the necessary granularity with a collection of periodical values (lower data actuality, typical for OMS LPWAN).

NOTE: A data actuality of e.g. 24 hours means that at least one time a day an update of the data in the AMMHES is provided.

It is recommended to transmit an update of consumption data with every synchronous transmission. However, the consumption data shall be updated at least with the update interval maximum as listed in Table 8.

Table 8 – Update interval of consumption data for billing

Device	Minimum data granularity [hours]	Update interval maximum [min] [a] for Mode C	Update interval maximum [hour] [b, c] for OMS LPWAN
Electricity	0,25	7,5	12
Gas	1	30	12
Heat (district heating)	1	30	12
Water / Warm water	24	240	12
Heat cost allocators	24	240	12
Heat / Cold (sub metering)	24	240	12
Repeater [c]	-	240	-

[a] Additional to this value a tolerance of +3,1258 % shall be accepted. This tolerance includes the scatter of the nominal transmission interval and an additional clock uncertainty of 250 ppm acc. to [EN 13757-4:2019], 12.6.2.
[b] The required data granularity can be achieved either with a smaller update interval or with providing the respective number of recent values, see formula (1).
[c] The values refers to data of the repeater itself. Not for repeated datagrams!

For consumer information that needs a high data actuality the UC-07 of Annex M can be supported. This use case provides a separate requirement for the consumption data update interval maximum.

The update interval maximum results from the aimed data actuality respecting a redundancy factor of 2. This redundancy factor is needed to guarantee a successful transmission for a typical reception probability of more than 95%. The aimed data actuality is 24 hours for OMS LPWAN. For Mode C it is identical to the minimum data granularity, e.g. 1 hour for a gas meter.

Due to the higher energy consumption of OMS LPWAN transmissions it makes sense to provide the necessary granularity with the collection of periodical values in one message using e.g. a Compact Profile (see Annex G). In this case the transmission of a related time stamp is required (see “DT1!P” in Annex B). The number of the necessary contained values (N_{DP}) depends on the selected update interval (T_U) and on the aimed data granularity (DG). It also shall take the redundancy factor (RF) into account. This results in the following formula (1):

$$\mathbf{N_{DP} = T_U / DG * RF} \qquad \mathbf{(1)}$$

Example:
A gas meter having a transmission interval of 12 hours (which is the allowed maximum) shall put N_{DP} = 12h / 1h * 2 = 24 values in each consumption data message.

A water meter that has to provide a (higher) data granularity of 1 hour with a transmission interval of 3 hours shall put N_{DP} = 3h / 1h * 2 = 6 values in each consumption data message.

4.3.2.3 Interval of Sensor Data

An update of sensor data with every synchronous transmission is recommended. However, the sensor data shall be updated at least with the update interval maximum as listed in Table 9.

See Table 9 for mandatory sensor data update periods:

Table 9 – Update interval of Sensor data for different devices

Device	Device-Type [EN13757-7:2023, 7.5.4]	Sub-Device-Type [EN13757-3:2023, 6.5.2]	Minimum data granularity [hours] [a]	Update interval maximum [min] [a] for Mode C	Update interval maximum [hours] [a, c] for OMS-LPWAN	Immediate update [b]
Humidity Sensor		1	1	30	12	change in RH1! >= 5%rH
Moisture Sensor		2	1	30	12	change in MO1! >= 5%
Temperature Sensor		3	1	30	12	change in TC4! >= 1°C
Light Sensor		5	1	30	12	% change in LT1! Or LT2! >= 10
Rainfall Sensor		6	1	30	12	change in RF1! >= 1 mm
pH Sensor		7	1	30	12	-
Anemometer		8	1	30	12	-
Glass Break Detector		9	1	30	12	-
Door/Window Contact Sensor		10	12	360	12	change in MM16!
Locked Door/Window Detector		11	12	360	12	change in MM16!
Water Leakage Detector		12	1	30	12	change in MM3! Bit10
Air Quality Sensor		13	1	30	12	change in VC1! >= 100µg/m³
CO_2 Sensor		14	1	30	12	change in CC2! >= 10ppm
Turbidity Sensor		15	1	30	12	% change in TB1! >= 10
CO Alarm Device	1Dh [d]	18	4	120	12	change in MM14!

Device	Device-Type [EN13757-7:2023, 7.5.4]	Sub-Device-Type [EN13757-3:2023, 6.5.2]	Minimum data granularity [hours] [a]	Update interval maximum [min] [a] for Mode C	Update interval maximum [hours] [a, c] for OMS-LPWAN	Immediate update [b]
Smoke Alarm Device	1Ah [d]	19	4	120	12	change in MM15!
Heat Alarm Device	1Eh [d]	20	4	120	12	change in MM17!
Pressure Device	18h [d]	21	1	30	12	change in MM13!

[a] Additional to this value a tolerance of +3,1258 % shall be accepted. This tolerance includes the scatter of the nominal transmission interval and an additional clock uncertainty of 250 ppm acc. to [EN 13757-4:2019], 12.6.2.
[b] Recommendation for an event-based trigger, in which the updated sensor data is sent within the next synchronous telegram.
[c] The required data granularity can be achieved either with a smaller update interval or with providing the respective number of recent values, see formula (1).
[d] Either the listed device type is used or the sub device type is used together with the device type 1Fh.

Data granularity, update interval maximum for mode C and update interval maximum for OMS-LPWAN are explained in 4.3.2.2.

4.3.2.4 Interval of Installation Data

The optional transmission of installation datagrams (with C = 46h) should happen only after a manual installation start event (e.g. push of installation button). Installation datagrams shall be transmitted according to [EN 13757-4:2019], 12.6.1. A SND-IR shall be sent within 60 s after the manual start event. Note that the duty cycle shall be respected also during installation mode. If the installation datagram contains fixed data for meter management (like OBIS code definitions, as defined in [EN 13757-3:2018] Annex H.3), it shall be marked as a static message (see [EN 13757-7:2019], Table 21).

4.3.2.5 Interval of Management Data

If an OMS end-device provides special management data (e.g. ownership number, OBIS definition codes or other data, which are not frequently changing), it can transmit this data in a static message. Static messages shall be marked as described in [EN 13757-7:2019], Table 21 and shall be sent at least with the maximum access opportunity delay according to Table 12 but not more than five times a day in a synchronous time slot to support battery driven receivers (e.g. battery driven repeater). The transmission of the static messages leads to a gap between the two adjacent SND-NR transmissions with dynamic data, which may lead to a larger update interval maximum (see Table 8 and Table 9). This will be accepted.

NOTE: It is not recommended to transport consumption data with a static message. But the definition of message content is manufacturer specific.

4.3.3 Access Timing of a Bidirectional OMS end-device

4.3.3.1 Access timing for Mode C2

An OMS end-device signals its own accessibility in the Link Control Bits (Bit B and Bit A in Table 10) of every transmission. These bits are located in either the Extended Link Layer (see 5.2.2.2) or the Configuration Field (security mode 0 and 5 only) (see 7.2.4.2 and 7.2.4.3). The OMS end-device initiates periodical transmissions. If the gateway wants to transmit a message to an OMS end-device, it checks the Link Control Bits whether the OMS end-device is accessible.

Table 10 – Accessibility of an OMS end-device

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

Unidirectional OMS end-devices (Mode C1) are never accessible. Therefore, unidirectional actuators are not allowed.

Mains powered OMS end-devices may provide an unlimited access and the gateway may send a command or a request at any time.
The communication partner (e.g., gateway, repeater or service tool) operating in Mode C2 shall also apply the bits B and A according the Table 10.

Battery operated bidirectional devices are very restricted in their power consumption. Typically, they will provide a short access window only immediately after a transmission. The gateway or any other communication device (as master) may initiate communication to the OMS end-device (as a slave) during this timeslot. The timing for Mode C shall in accordance with [EN 13757-4:2019], clause 9. For Mode C2 the standard defines two response delays: t_{RO} and t_{RO_slow}, which are selected by the Response Delay Subfield (D-field) in the communication control field of the extended link layer (refer to 12.2.2 in [EN 13757-4:2019]). The stationary gateway shall always select D = 0. The OMS end-device may start the communication with any value of subfield D.

The response delay t_{RO} respectively t_{RO_slow} shall be calculated from the end of the OMS end-device transmission to the start of the gateway transmission. The transmission of the first chip (bit) of the preamble shall start before the maximum delay of t_{RO} respectively t_{RO_slow} expires and the OMS end-device shall then receive the transmission from the gateway or another device correctly.

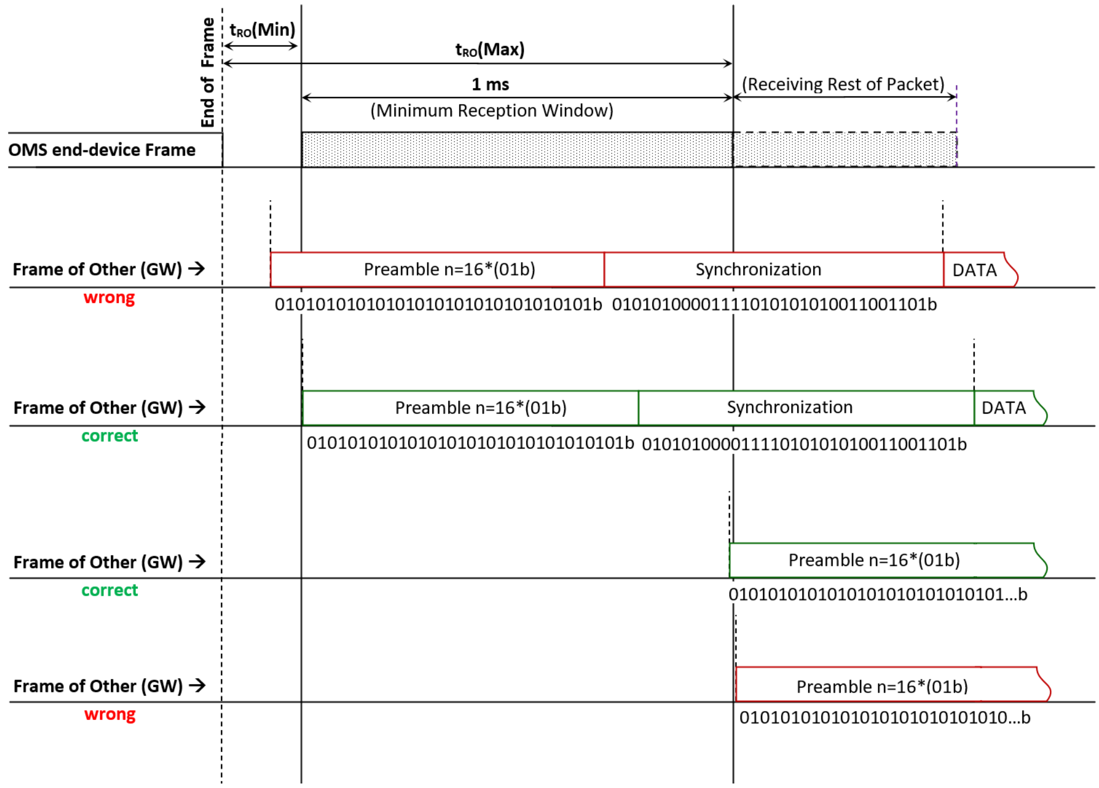


Figure 17 – Access timing of an OMS end-device with short access windows (Mode C2 example)

Figure 17 shows examples for both correct and wrong access timing to an OMS end-device device. The start of the minimum preamble according to [EN 13757-4:2019] shall fall within the minimum reception window of the receiver.

4.3.3.2 Access timing for OMS-LPWAN

For OMS LPWAN the Link Control Bits are located in the MElements of the MAC-Layer and are called Downlink accessibility (see Annex Q, Q.3.5). The OMS end-device initiates periodical transmissions. The OMS end-device is typically battery operated and can provide (one or several) short reception windows after a transmission. If the gateway wants to transmit a message to an OMS end-device, it checks the access options in the MElements-field, whether the OMS end-device is accessible and at which time. OMS LPWAN supports several access options with different delays for the response time (see Annex Q, Q.2.4.6 and Q.2.5.6).

The OMS LPWAN also support special “access option” values for unidirectional OMS end-devices (with no access windows) and for permanent access applicable for mains powered OMS end-devices.

Further details are provided in Annex Q.

4.3.3.3 Frequent Access Cycle

Bidirectional OMS end-devices operating in Mode C shall support the Frequent Access Cycle as defined in [EN 13757-4:2019], 12.6.3.3.

Bidirectional OMS end-devices using OMS LPWAN support a special downlink communication session (see Annex Q, Q.3.3.5) to resume an unintended interrupt of a bidirectional communication session.

4.3.4 Transmissions Limits and Transmission Credits

An OMS end-device has a nominal transmission interval (refer to 4.3.2.1 and [EN 13757-4:2019], 3.12). This results in a nominal number of transmissions (transmitted datagrams) per day. Bidirectional devices offer the possibility to request/send additional transmissions from/to the OMS end-device. The number of additional transmissions is controlled by the gateway.

Battery powered devices are limited in their power consumption. Mains and battery powered devices are limited by the duty cycle. For that reason, it may happen that the OMS end-device has to stop communication, if the gateway or another communication unit sends too many commands or requests. To handle this issue every bidirectional OMS end-device needs to manage additional radio transmissions in terms of power consumption and duty cycle.

In addition to its unidirectional transmission scheme (see 4.3.2), a bidirectional OMS end-device shall provide a minimum of bidirectional communication capability. This is managed by so-called credits. The number of credits per message type is given in Table 11.

Table 11 – Credits per datagram

Messages for bidirectional communication	Credits per datagram
Receive a SND-UD, SND-UD2 [b]	2
Receive a REQ-UD1, REQ-UD2, SND-NKE, CNF-IR [b]	1
Receive a pure OMS LPWAN MAC layer message [c]	1
Transmit a RSP-UD [b]	5
Transmit an ACK, NACK [b]	1
Transmit a SND-NR, ACC-NR, ACC-DMD, SND-IR [a, b]	0
Transmit a pure OMS LPWAN MAC layer message [c]	1

[a] The transmission of these message types is not initiated by the gateway and has not to be considered as credits for a bidirectional communication. However, it needs to be considered in the power budget calculation for unidirectional communication, which is not in the scope of the credit handling specified in this subclause.
[b] Message types according to **5**.2.3
[c] According to Annex Q

NOTE: The credits are intentionally not reflecting the exact energy consumption of different radio technologies but are designed for a harmonized usage of the interface in a gateway or backend.

The OMS end-device shall manage a credit counter that is decremented by the given number of credits whenever the OMS end-device transmits or receives a datagram with its own address (see 3.1). The OED shall treat a message with unknown C-Field (message type unclear) like a SND-UD.

NOTE 1: To save credits the gateway needs to terminate the session (see 5.2.6).

The credit counter shall be decremented before sending a datagram. If the credit counter becomes less than zero, it shall be set to zero. In case the credit counter becomes zero or the duty cycle limit exceeds, the OMS end-device is not able to receive further datagrams and shall mark this state by the Link Control Bits (see Table 10 for Mode C and Annex Q, Q.3.5.1.1, for OMS LPWAN) of this last datagram and every following spontaneous transmitted datagrams. During this period a gateway has no access to the OMS end-device. As soon as bidirectional communication is available again, the OMS end-device shall mark this accessibility by the Link Control Bits in the next transmissions. The OMS end-device shall enable bidirectional communication again at least after the maximum access opportunity delay of Table 12. The delay is measured from the first transmission without access to the first transmission with access opportunity.

Table 12 – Maximum access opportunity delay

Radio mode	Delay in hours
Mode C	12
UL-B4	24
UL-B1...B3	48
UL-S1…S3	72

If an OMS end-device runs into the limit of its duty cycle, it will omit sending any asynchronous datagram (see 4.3.2.1). The usage of duty cycle for unidirectional transmissions shall allow a minimum number of credits as defined in Table 13 for bidirectional communication.
An OMS end-device shall increase the credit counter at least as defined in Table 13.

Table 13 – Minimum credits per radio mode

Radio mode	Minimum available credits within duty cycle per 2 hours	Minimum credit counter increase per 2 hours
Mode C	240	10
UL-B4	240	5
UL-B1...B3	120	2
UL-S1…S3	120	1

The OMS end-device shall accumulate unused credits at least up to 4000 credits. It may accumulate more.

The OMS end-device may interrupt the communication after having used 240 credits within 12 hours, even if the credit counter > 0 or the duty cycle limits are not exceeded. The OMS end-device shall enable bidirectional communication again not later than defined in Table 12 after the first transmission without access.

NOTE 2: The OMS end-device can apply this rule to protect itself against surplus usage of credits.

An OMS end-device that supports a software update via radio (see Annex M.2.6) shall provide sufficient battery power for one or several software updates during its lifetime. The number of possible firmware updates shall be declared in the data sheet. The power budget for this use case must be assigned in addition to the "regular" bidirectional communications as described above.

NOTE 3: If the operator performs more firmware updates than indicated in the data sheet, the lifetime of the device may be reduced.

Once the firmware update has started, it shall not be interrupted due to the credit management of a bidirectional communication as described above. The firmware transfer procedure is started after the reception of a "Synchronise command" or "Transfer command" and is finished after the reception of a "Validate command" or "Terminate command" (see [EN 13757-3:2018], Annex I).

NOTE 4: The activation of the new firmware may be some time after the firmware transfer. For that reason, the activation command is not considered a part of the firmware transfer procedure.

If an OMS end-device needs to limit the number of communications on another interface (e.g. optical interface), it shall apply an additional power budget management, which is independent of the one for the radio interface.

5 Link Layer

5.1 Wired Communication (Wired M-Bus)

The Link Layer is fully described in [EN 13757-2:2018] and Annex P. The requirements for the addressing of wired M-Bus devices are described in subclause 3.1.2 of [EN 13757-2:2018]. Wired M-Bus devices shall support datagrams with an L-Field ≤ 255.

The Link Layer itself does not support multi-datagram messages. Functions requiring more data than the maximum length of a datagram may handle a fragmentation of long messages via the Authentication and Fragmentation Layer (see clause 6).

The Annex N of this specification contains examples of wired M-Bus-datagrams.

5.2 Wireless Communication (Wireless M-Bus)

5.2.1 General

The Link Layer applies different frame formats depending on the mode. The Data Link Layer with Frame Format A as described in [EN 13757-4:2019] shall be used for wireless communication in Mode C. For wireless communication in OMS LPWAN, the Link Layer with Frame Format C (see 5.2.3) shall be used instead.

After the Data Link Layer, a CI-Field introducing structure and length of the next layer follows. Such a next layer can be the Authentication and Fragmentation Layer, a Transport Layer (with or without Application protocol) or in Frame Format A the Extended Link Layer (see 5.2.2.2).

Link Layer encryption (provided by the ELL) shall not be applied to any of the frame formats. The requirements to the addressing of wireless M-Bus devices are described in subclause 3.1.3.

The Link Layer itself does not support multi-datagram messages. Functions requiring more data than the maximum length of a datagram shall handle a fragmentation of long messages via the Authentication and Fragmentation Layer (see clause 6).

The Annex C of the [EN 13757-4:2019] contains datagram examples from the application data down to a bit stream. See also Annex N of this specification for examples of different message types. For datagram examples in Frame Format C, see Annex Q, Q.K.

5.2.2 Frame Format A

5.2.2.1 Data Link Layer

In Frame Format A, the Data Link Layer as described in [EN 13757-4:2019] shall be used. It shall be used in case of the wireless M-Bus Mode C and has a fixed length of 10 bytes (without CRC). It includes the datagram length (L-Field) (see 5.2.2.1.1), the C-Field (see 5.2.4) and the transmitter address (Link Layer Address). Integrity validation is done in blocks.

5.2.2.1.1 L-Field (Datagram-Length)

The L-Field shall be according to [EN 13757-4:2019], 12.5.3.

A bidirectional OMS end-device shall be able to receive datagrams with an L-Field ≤ 155.

OMS end-devices providing Security profile C (see Table 43) or a Software update over the air shall support datagrams with an L-Field ≤ 255.

5.2.2.2 Extended Link Layer

5.2.2.2.1 General

The Extended Link Layer (ELL) is defined in [EN 13757-4:2019] as an extension of the regular Link Layer. The Extended Link Layer shall be applied for wireless M-Bus only.

5.2.2.2.2 Structure of the Extended Link Layer (ELL)

There is a short and long Extended Link Layer. The long ELL provides an additional address field (see 3.1.3 and 3.1.5).

NOTE: The [EN 13757-4:2019] supports additional types of Extended Link Layers, which are not supported by the OMS.

CI = 8Ch	CC	ACC

Figure 18 – Short ELL without receiver address

CI = 8Eh	CC	ACC	Manuf.	Ident. no	Ver.	Dev.

Figure 19 – Long ELL with receiver address

Legend:

CC	Communication Control Field (see 5.2.2.2.3)
ACC	Access number (see 7.2.2.1)
Ident. No	Identification Number (part of receiver address)
Manuf.	Manufacturer ID (part of receiver address)
Ver.	Version (part of receiver address)
Dev.	Device Type (part of receiver address)

5.2.2.2.3 The Communication Control Field (CC)

The Communication control field uses the structure as shown in Table 14.

Table 14 – Definition of the Communication Control Field (CC)

MS Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	LS Bit 0
Bidirectional communication	Delay	Synchronous	Hop Counter	Priority (always 0)	Accessibility	Repeated Access	Reserved (always 0)
B	D	S	H	0	A	R	0

The link control bits B, A, S, R, H are also present in the Configuration Field, if security mode 0 or 5 is selected (see 7.2.4.2 and 7.2.4.3). In the case that both the CC-Field and the Configuration Field in the datagram exist, only the link control bits of the CC-Field shall be applied and the link control bits of the Configuration Field shall be ignored.

The bit S shall be used as described in subclause 4.3.2.1.

The bits B and A shall be used as described in subclause 4.3.3.1.

The bit D shall be used as described in subclause 4.3.3.1.

The bit H is used as a Hop Counter to indicate a repeated transmission. The OMS end-device, or gateway shall always transmit bit H = 0b. The bit R is reserved for use in repeated messages. The OMS end-device shall always transmit bit R = 0b. An OMS end-device may ignore a received bit R.

5.2.2.2.4 Condition to Apply the Extended Link Layer

The Extended Link Layer shall always be applied for mode C message types. There is one exception due to downward compatibility to former OMS specifications. A unidirectional OMS end-device that only uses Security Mode 5 (and 0) can omit the ELL for all applicable message types (SND-NR; SND-IR or ACC-NR). A mixture of using and not using the ELL is not allowed.

NOTE: Without using the ELL it is not possible to transmit new data with asynchronous transmissions (see 7.2.2.1).

The usage of the ELL may also be applied for security mode 5 in the case of an OMS end-device with internal encryption function and an external RF-Adapter. Both functions, the security mode 5 and the generation of synchronous transmissions, use and increment the Access number. For that reason, two Access Numbers are necessary.

Typically, the usage of the short ELL is sufficient. Special cases that require the long ELL are described in subclause 3.1.3.3.

5.2.3 Frame Format C

OMS LPWAN applies the Link Layer with Medium Access Control (MAC) and Logical Link Control (LLC) sublayers of flexible length. The LLC always applies the Frame Format C as described in Annex Q, Q.4. The MAC layer shall be applied according to Annex Q, Q.3.

5.2.4 Supported C-Fields

The C-Field is used to declare the message types. It is in conformance with the unbalanced C-Fields of [EN 60870-5-2].

There are different message types for data exchange:

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

The message type is indicated by the C-Field.

The following C-Fields may be generated by the master (gateway or other communication device) and shall be accepted by the slave (OMS end-device).

Table 15 – C-Fields of master (gateway or other communication device)

Message types of master	C-Fields (hex)	Explanation	Message types of responding slave
SND-NKE	40h	Link reset after communication; Also signals that after reception of an installation datagram it is capable to receive this OMS end-device	-
SND-UD2 [b]	43h	Send command with subsequent response (Send User Data - 2nd message type)	RSP-UD, NACK
SND-UD [a]	53h, 73h	Send command (Send User Data)	ACK, NACK
REQ-UD1 [a]	5Ah, 7Ah	Alarm request, (Request User Data Class1)	ACK, RSP-UD
REQ-UD2 [a]	5Bh, 7Bh	Data request (Request User Data Class2)	RSP-UD
ACK	00h	Acknowledge to the reception of the ACC-DMD	-
CNF-IR	06h	Confirms the successful registration (installation) of OMS end-device into this gateway	-

[a] The use of bits FCB, FCV should be in accordance with [EN 60870-5-2] [5]
[b] The SND-UD2 shall not be used for fragmented messages.

Only the message type SND-UD and SND-UD2 can be applied to transport application data to an OMS end-device.

The OMS end-device may send spontaneously or as a reaction to a gateway-datagram the following message types:

Table 16 – C-Fields of slave (OMS end-device)

Message types of slaves	C-Fields (hex)	Explanation	Message types of responding master
SND-NR [b]	44h	Send spontaneous/periodical application data without request (Send/No Reply)	-
SND-IR	46h	Send manually initiated installation data (Send Installation Request)	CNF-IR, SND-NKE [d]

[5] The Master is requested to apply FCB accordingly. The slave will ignore FCB. It uses the Access number only for the identification of an old/new message (see 7.2.2.1).

Message types of slaves	C-Fields (hex)	Explanation	Message types of responding master
ACC-NR	47h	Contains no data – signals an empty transmission or provides the opportunity to access the bidirectional OMS end-device between two transmissions of application data.	-
ACC-DMD	48h	Access demand to master in order to request new important application data (alerts)	ACK
ACK [a]	00h, 10h, 20h, 30h	Acknowledge the reception of a SND-UD (acknowledgement of transmission only); It shall also be used as a response to an REQ-UD1, when no alert happened	-
NACK [c]	01h, 11h, 21h, 31h	Replace an ACK in the case of a persistent Link Layer error: • OMS end-device reception buffer overflow • Master datagram with invalid or unknown C field	-
RSP-UD [a]	08h, 18h, 28h, 38h	Response of application data after a request from master (response of user data)	-

[a] The use of bits ACD and DFC shall be in accordance with [EN 60870-5-2]
[b] The SND-NR shall be used in wireless M-Bus only and not for fragmented messages.
[c] NACK datagram shall not contain any error codes. A NACK datagram shall only be sent if the check of the CRC-tested destination address of the received message has been passed. **NOTE:** A CRC-error is not a persistent Link Layer error.
[d] SND-NKE is in this case not a direct response to the OMS end-device but an information to third party like a service tool to signal an available radio link

Only message types RSP-UD and SND-NR can be applied to transport application data from an OMS end-device to the gateway. SND-IR should be applied to transport application data for installation and management purposes only. If an OMS end-device does not support alarm functions it shall acknowledge a REQ-UD1 with an ACK. Otherwise it shall react according to [EN 13757-3:2018], Annex D.

Uni- and bidirectional OMS end-devices shall support the message type SND-NR. Optionally SND-IR (for the support of a tool-less installation mode for gateways without external installation support) and ACC-NR (see 4.3.2.1) may be supported by the OMS end-device.

The slave shall reply to every datagram of the master with an expected response, according to Table 15 independently of whether this datagram was already received earlier (see 7.2.2). Exceptions to this rule are described in subclauses 4.3.3 and 4.3.4. The timing and interaction between different message types are shown in Annex L.

5.2.5 Repeater for the Wireless Communication

5.2.5.1 General

If a direct wireless transmission between an OMS end-device and a gateway is not possible, a single intermediate repeater might be used. Such a repeater shall be able to work without complex installation procedures and without routing capability. For a common device management, a repeater shall send datagrams with its own address to provide device management data like status. A repeater conforms to general rules like every OMS end-device. The repeater shall send this data periodically (see Table 8). It may optionally send installation datagrams (with C = 46h) within given time limits (see 4.3.2).

A repeater may be a dedicated device or a function integrated into an OMS end-device or a gateway. An integrated repeater should use the address of the hosted OMS end-device or the gateway. Both integrated and dedicated repeaters shall apply the Device Type “unidirectional repeater” or “bidirectional repeater” (Table 3) for the transmission of repeater management data.

It will be distinguished between:

- Unidirectional repeaters (repeat datagrams from the OMS end-device upward to the gateway only)
- Bidirectional repeaters (repeat datagrams in both directions; from the OMS end-device upwards to the gateway, and from the gateway downwards to the addressed OMS end-device)

5.2.5.2 Unidirectional Repeater

The unidirectional repeater repeats only datagrams with C-Fields C = 46h or C = 44h. All other datagrams shall be ignored.

It just retransmits (with some delay) a received Open Metering System compatible datagram only in case of Hop Counter Bit = 0 and Repeated Access Bit = 0. The Hop Counter Bit (bit H) and Repeated Access Bit (bit R) are placed either in the CC-Field of the Extended Link-Layer (see 5.2.2.2.3 and 5.2.2.2.4) or in the Configuration Field in the Transport Layer (see 7.2.4.2 and 7.2.4.3). In OMS LPWAN, the Hop Counter Bit is placed in the LC[1] field of Frame Format C (see Annex Q, Q.4.2.2) instead of the ELL. The repeater shall increment the Hop Counter Bit to 1 before the retransmission, what requires the recalculation of the CRC value for the second block. Datagrams that do not provide a Hop Counter Bit shall be ignored.

The retransmission should be randomly delayed for at least 5 seconds and no longer than 25 seconds after reception time. Due to this delay it is not possible to calculate accurately the actual consumption (power, flow) based on the difference of the index values of subsequent datagrams. Also, the transfer of the OMS end-device time will not be accurate.

If the repeater receives an installation datagram (with C = 46h) with a Hop Counter = 0 it shall additionally generate a SND-NKE message to confirm the ability of receiving this OMS end-device to an optional installation service tool. This message shall be generated with a reaction delay between 2 and 5 seconds after retransmission of the OMS end-device message. The installation procedure with repeater is shown in Annex L.

Note that the repeater itself is responsible for staying within duty cycle limits and off time limits in any case.

5.2.5.3 Bidirectional Repeater

A fully functional bidirectional repeater will be defined in a separate volume of the OMS specification.

5.2.6 Rules for the Gateway

If the gateway receives an installation datagram with C = 46h and with a Hop Counter = 0 it shall generate a SND-NKE to confirm the ability to receive this OMS end-device to an optional installation service tool. This message shall be generated within a random delay between min. 5 and max. 25 seconds after the direct reception of an OMS end-device installation datagram. In addition, it may generate a CNF-IR message to the OMS end-device or an optional installation service tool to signal its assignment to this gateway.

In case of an erroneous multiple assignment of one OMS end-device to several gateways, collisions may happen when more than one gateway accesses an OMS end-device. To solve this failure every gateway shall support a collision avoidance mechanism as defined in Annex I. This mechanism describes a random-access taking effect after the second unsuccessful access attempt to an OMS end-device.

If the gateway finishes a communication session with a bidirectional OMS end-device in radio Mode C it shall apply a SND-NKE message to stop the Frequent Access Cycle (see 4.3.3.3) of the OMS end-device. In OMS LPWAN, OMS end devices don't apply the Frequent Access Cycle. In this case, the gateway shall finish the communication session with a set Session Control bit (SC) in MElement_DA in the last downlink frame (see Annex Q, Q.3.3.5).

The gateway shall provide a clock synchronisation service (see 8.7), unless otherwise specified in Annex E. In OMS LPWAN, the MAC layer provides a service for clock management (see Annex Q, Q.3.7.2).

The gateway shall support datagrams with maximum length (L-Field ≤ 255).

6 Authentication and Fragmentation Layer

6.1 General

This section specifies rules for the usage of the Authentication and Fragmentation Layer (AFL) as specified in [EN 13757-7:2018, clause 6] in combination with the other layers and security modes used in OMS.

6.2 Rules for Specific AFL Fields

6.2.1 AT-Subfield of AFL.MCL

OMS end-devices and gateways shall use the value 5 for the AT-subfield (AES-CMAC-128, 8 bytes).

Gateways should also support the values 6 and 7 for the AT-subfield (AES-CMAC-128, 12 and 16 bytes) to be future-proof.

6.2.2 AFL.KI

OMS end-devices shall support an internal flag, called KI-Flag, to control the presence of the KI-Field. The KI-Flag is cleared by default. If a gateway or any other communication partner applies AFL-Key Information Field (AFL.KI) in SND-UD or SND-UD2, then the OMS end-device shall set the KI-Flag. Otherwise, it shall clear the KI-Flag. The AFL.KI shall be present in RSP-UD as long as the KI-Flag is set. In case of a fragmented response and an enabled KI-Flag, the AFL.KI field shall be present in the first fragment. It should not be present in any following fragments of the same message.

6.2.3 AFL.MCR

The AFL.MCR shall be present in messages from/to OMS end-devices that are protected by Security profile B. It is also required for selected messages of Security profile C (see Annex F). See 9.2.5 for details on the requirements for the message counter.

6.2.4 AFL.MAC

If the MAC-Field is used, the AFL.MAC field shall only be present in the last fragment of a message, i.e. the entire message shall be authenticated.

NOTE: OMS supports only the authentication of the complete message. Therefore, the MAC is only present in the last fragment.

6.2.5 AFL.ML

The message length shall be limited to 16 kbytes.

For unfragmented messages, the AFL.ML shall not be used.

6.3 Conditions to Apply an AFL

The AFL shall be applied

- In each datagram of a fragmented message (SND-UD, RSP-UD)
- In message types with application data (SND-NR, SND-UD, SND-UD2, SND-IR, RSP-UD) using Security profile B (see 9.1)
- In each RSP-UD message, when KI-Flag is set (see 6.2.2)
- In selected messages using Security profile C (see 9.1) with CMAC (see Annex F, F.3.4)

If the AFL is used, the rules specified in 6.2 shall apply.

If the required AFL is missing or wrong in SND-UDx messages the OMS end-device shall provide an application error (see 8.8).

7 Transport Layer

7.1 Overview

The Transport Layer always has a fixed frame structure as described in [EN 13757-7:2018]. It may transport either the OMS end-device Application Protocol according to [EN 13757-3:2018] (M-Bus), or alternatively [EN 13757-1:2014] (DLMS/COSEM communication primarily used by electricity meters). Note that the CI-Field as the first byte of the Transport Layer distinguishes between these Application Protocol types and the frame structure. A gateway or a consumer display shall be able to handle all Application Protocol types at least to the extent that it can extract the values required for its function or application from the message. This specification part covers mainly the M-Bus variant.

NOTE: The gateway or the display needs to be able to parse any applied (M-Bus or COSEM or SML) Application Protocol into separate data points. However, it is sufficient to "understand" i.e. decode only the required values stated in clause 8.

7.2 Common Part for All Transport Layers

7.2.1 General Structure of the Transport Layer

The frame format of the Transport Layer is the same for all Application Protocols. The Transport Layer starts with a CI-Field (see 2.2), which indicates the main message function and the type of coding (i.e. the Application Protocol) used for the rest of the message. After the CI-Field a fixed sequence of bytes follows, which is called TPL-header. There are three types of TPL-headers.

The TPL-header structures are:

- No TPL-header:
  This TPL-header type is used on the wired M-Bus for unencrypted messages. The next byte after the CI-Field is the first byte of the selected Application Protocol.
- Short TPL-header:
  The Short TPL-header is used only for wireless M-Bus. If the message contains such a "short" TPL-header, the OMS end-device identification is taken from the Link Layer (see 3.1.3.1 and 3.1.4.2).
- Long TPL-header:
  The Long TPL-header is used for both wired and wireless M-Bus. If the message contains such a "long" TPL-header, this TPL-header always contains (independent of transmission direction) the OMS end-device identification (see 3.1.3.4 and 3.1.4.4). The long TPL-header enables encrypted messages on the wired M-Bus.

Every Short/Long TPL-header for wireless M-Bus contains:

- Access number
- status byte
- Configuration Field

Depending on the selected security mode in the Configuration Field, additional bytes (like Configuration Field Extension or Decryption-Verification) may follow before the Application Protocol starts. The structures of the Transport and Application Layer is pictured in Annex D. Table 1 in subclause 2.2 lists all supported CI-Fields and the related TPL-header types.

7.2.2 Access Number

7.2.2.1 Access Number for Wireless M-Bus

The Access Number together with the transmitter address is used to identify a datagram. It will be distinguished between:

- OMS end-device Access Number
- Gateway Access Number

The OMS end-device Access Number is generated by the OMS end-device. It shall be incremented by 1 (and only 1) with every synchronous transmission (see 4.3.2.1). Asynchronous transmissions shall always apply the OMS end-device Access Number of the last synchronous transmission. The OMS end-device Access Number shall be applied to SND-NR, SND-IR, ACC-NR and ACC-DMD datagrams. If a gateway accepts an ACC-DMD or a SND-IR from an OMS end-device, it has to send an acknowledgement (ACK or CNF-IR) using the received OMS end-device Access Number. The received Gateway Access Number has no impact on the stored OMS end-device Access Number of the OMS end-device. After power-up of the OMS end-device the value of the OMS end-device Access Number shall be set to a randomized initial value from 0 to 255. The OMS end-device Access Number shall not be resettable.

An access number in the link layer (LL-ACC) can either be provided in Frame Format C (LLC-ACC) or in the Extended Link Layer (ELL-ACC) in case of Frame Format A. If an LL-ACC exists, it shall be used for the synchronous transmission and Link acknowledgement. Each datagram can be identified by the LL-ACC. In case the LL-ACC does not exist (i.e. for Security Profile A) the TPL-ACC shall be used for synchronous transmission.

The additional Access Number of the Transport Layer (TPL-ACC) may differ from the LL-ACC. This TPL-ACC shall be used to indicate a new or old message content. Each message can be identified by the TPL-ACC. The (first) response (RSP-UD) of a (fragmented) message shall contain the TPL-ACC of the concerning request (REQ-UD2) and the (last) acknowledgement (ACK) of a (fragmented) message shall contain the TPL-Access Number of the concerning command (SND-UD). Other acknowledgement datagrams of a fragmented message may contain a Transport Layer (with the TPL-ACC) e.g. to provide an application error bit in the status byte.

The relation of the Access Number terms is shown in Figure 20.

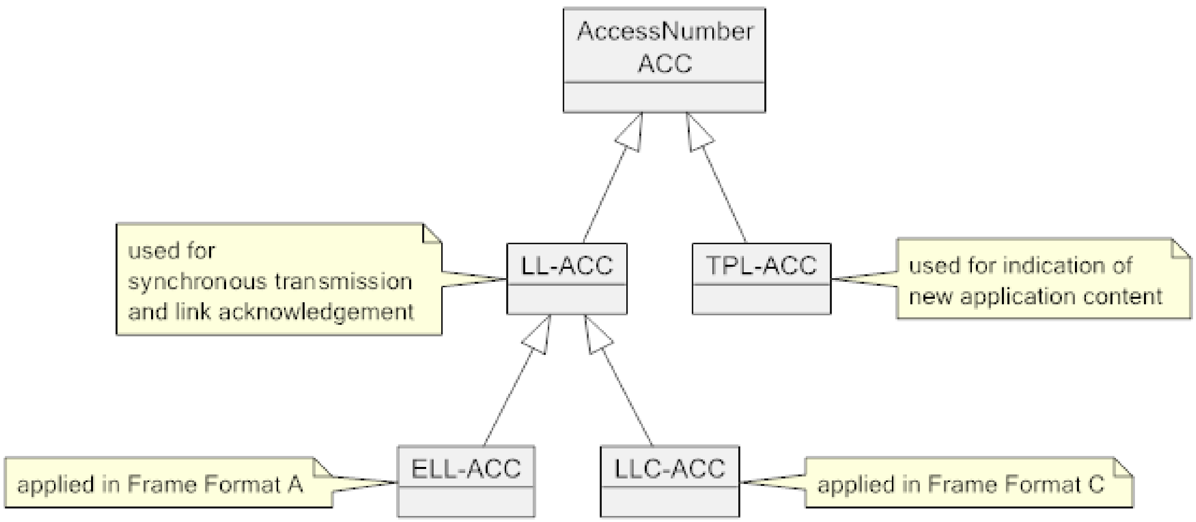


Figure 20 – Access Number

The Gateway Access Number is generated by the gateway. It may be selected without any restrictions. However, the gateway shall not use the same Gateway Access Number for a new datagram to the same OMS end-device again within 300 seconds. Each time the Gateway Access Number is changed, the gateway should alternate the FCB (see 5.2.4).

The OMS end-device shall not expect any specific order of Gateway Access Numbers in datagrams received from the gateway. It shall only distinguish between a new and an old datagram. The last received Gateway Access Number marks an old datagram. All other Gateway Access Numbers different from the last received one will be handled as the new Gateway Access Number. The content of the FCB (see 5.2.4) shall be ignored. When the OMS end-device finishes the Frequent Access Cycle (see 4.3.3) or closes the downlink communication session (see Q.3.3.5), it shall clear the last received Gateway Access Number. After that any received Gateway Access Number will be handled as a new one.

If the OMS end-device receives an SND-NKE, SND-UD, SND-UD2, REQ-UD1, or REQ-UD2, it shall use the received Gateway Access Number of the LL-ACC for its response or acknowledgement. The gateway may recognize an outstanding response or acknowledgement by its own Gateway Access Number. Hence the OMS end-device repeats the last response or acknowledgement, if the gateway has sent the request or the command with the old LL-ACC again. Otherwise, it shall generate a new datagram with the new LL-ACC received from the gateway.

NOTE: These rules to apply the Access number for wireless M-Bus is in accordance with [EN 13757-7:2018].

7.2.2.2 Access Number for Wired M-Bus

For wired M-Bus the Access Number shall be in accordance with [EN 13757-7:2018], 7.5.5.

7.2.3 Status Byte

The status byte shall be applied as defined in [EN 13757-7:2018]. It will be distinguished between the OMS end-device status (see [EN 13757-7:2018], 7.5.6) and gateway status (see [EN 13757-7:2018], 7.5.7).

In a 2-way communication, the OMS end-device shall indicate in the status byte its application status within an ACK or RSP-UD message. Table 17 provides the three application states coded in the lowest two bits of the status byte (according to [EN 13757-7:2018], 7.5.6, Table 15 – Application errors coded with the status field) to reflect the state of the command response (see 8.2.5). It also shows the fourth possibility, which is limited to self-initiated messages.

Table 17 – Application error bits in OMS end-device status byte

Status Bit 1	Status Bit 0	Command state	Usage
0	0	No error [a, d]	Shall be used if the last command was processed successfully and complete without any issue.
0	1	Application busy [b, d]	Shall be used as default response as long as no positive or negative feedback to the last command has been received from the (internal) application.
1	0	Any application error [c, d]	Shall be used, if a problem was detected in terms of authentication check, decryption, interpretation, or execution to the last command. The RSP-UD provides an Error Response (see 8.2.5).
1	1	Abnormal condition/ alarm	Shall not be used as a reaction to a command. It can be used in self-initiate push messages or in normal data response states (see 8.2.3).

Status Bit 1	Status Bit 0	Command state	Usage

[a] If a "Command Successful" (see 8.2.5) was used the gateway does not need to send a REQ-UD2.
[b] The gateway should request the “final” status with another REQ-UD2 (using a new TPL-ACC).
[c] The gateway should send a REQ-UD2 if the bit combination "any application error" is set to read back the application error.
[d] Note that older OMS end-devices may not support these application error bits and always use "00b".

Annex L.5 shows a sequence diagram that illustrates the three possible command response states.

The state of the application error bits in status byte shall be updated whenever a new application response is generated. Subclause 8.2.5 shows, which events change the application response.

NOTE: During the datagram repetition within the FAC (see 4.3.3.3) the status byte will not be updated.

It is recommended, that the Low Power bit is set 15 months before the intended end of operation.

Details about other error conditions like "permanent error" may be provided in an Application Protocol (see 8.4.5.2).

7.2.4 Configuration Field

7.2.4.1 General

The Configuration Field shall be used as specified in [EN 13757-7:2018]. It declares the method of data encryption (security mode) and the length of encrypted data. The security mode is a part of the Configuration Field declared by the bits MMMMM. The security mode also determines the presence of the Configuration Field Extension and the meaning of all other bits (see 7.2.4.7).

NOTE 1: In former OMS-Specifications the Configuration Fields for security modes 7 and 13 were presented as a 3-byte field. According to [EN 13757-7:2018] the Configuration Field is limited to two bytes. Additional bytes are called Configuration Field Extension (CFE) and are presented separately. Nevertheless, the byte order in the message is the same.

Table 18 shows the general structure of the Configuration Field and the position of the security mode.

Table 18 – General definition of the Configuration Field

MS Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	LS Bit 0
Mode specific	Mode specific	Mode specific	Mode bit4	Mode bit3	Mode bit2	Mode bit1	Mode bit0	Mode specific	Mode specific	Mode specific	Mode specific	Mode specific	Mode specific	Mode specific	Mode specific
X	X	X	M	M	M	M	M	X	X	X	X	X	X	X	X

NOTE 2: In [OMS-S2]. Issue 3.0.1 the applied Mode Field includes only bit 8 to bit 11. Bit 12 was marked as reserved. From [OMS-S2] Issue 4.0.2 on the Mode Field includes the bits from bit 8 to bit 12.

For OMS only the following security modes shall apply:

- Security mode 0 (no encryption)
- Security mode 5 (OMS standard for symmetric encryption)
- Security mode 7 (OMS standard for advanced symmetric encryption)
- Security mode 10 (OMS standard for advanced symmetric authenticated-encryption)
- Security mode 13 (OMS standard for asymmetric encryption)

Subclause 9.3 describes the usage of these security modes. The next sub-sections describe the structure of the mode specific Configuration Fields.

7.2.4.2 Configuration Field for Security Mode 0

The structure of the Configuration Field of Mode 0 is identical to security mode 5 (see Table 19). The M and N bits have to be set to 00h to indicate that no encryption is applied. See also subclause 9.3.4.

7.2.4.3 Configuration Field for Security Mode 5

Security mode 5 is a symmetric encryption method using AES128 with CBC, a special initialisation vector, and a persistent key (see 9.3.5).

Table 19 – Definition of the Configuration Field for security mode MMMMM = 5

MS Bit 15	**Bit 14**	**Bit 13**	**Bit 12**	**Bit 11**	**Bit 10**	**Bit 9**	**Bit 8**	**Bit 7**	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**LS Bit 0**
Bidirectional Communication	Accessibility	Synchronous	Mode bit4	Mode bit3	Mode bit2	Mode bit1	Mode bit0	Number of encr. blocks	Number of encr. blocks	Number of encr. Blocks	Number of encr. blocks	Content of Message	Content of Message	Repeated Access	Hop Counter
B	A	S	M	M	M	M	M	N	N	N	N	C	C	R	H

M is always 05h to mark AES128 with CBC and persistent key.

N contains the number of encrypted 16-byte blocks for CBC Mode. An N of 1111b specifies that partial encryption is disabled and no unencrypted data follows after the encrypted data. This enables the possibility to encrypt very large fragmented messages. If N is set to 0000b, no encrypted data follows.

C declares the Content of Message (see 7.2.4.7).

B, A, S, R, and H are used to control the link (see 7.2.4.8).

A two-byte sequence 2Fh, 2Fh (decryption verification) shall immediately follow the Configuration Field. The Decryption Verification Field is part of the Transport Layer.

NOTE: The Mode 5 may be used without Extended Link Layer and without Authentication and Fragmentation Layer (see 5.2.2.2.4).

7.2.4.4 Configuration Field for Security Mode 7

Security mode 7 is a symmetric encryption method using AES128 with CBC and an ephemeral key (see 9.3.6). It is possible to identify up to 16 different communication security keys using the KeyID.

The Configuration Field (CF) to be used for security mode 07h is defined as follows:

Table 20 – Configuration Field for security mode 7

MSBit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	LSBit 0
Content of Message	Content of Message	Reserved for Counter Size	Mode 4	Mode 3	Mode 2	Mode 1	Mode 0	Number of encr. blocks	Number of encr. blocks	Number of encr. blocks	Number of encr. blocks	Padding	Content Index	Content Index	Content Index
C	C	0	M	M	M	M	M	N	N	N	N	P	I	I	I

M is always 07h to mark AES128 with CBC and ephemeral key.

C declares the Content of the Message, I declares the Content Index (see 7.2.4.7).

P is the padding bit according to [EN 13757-7:2018], 9.4.5.4.

N contains the number of encrypted 16-byte blocks for CBC Mode. An N of 1111b specifies that partial encryption is disabled and no unencrypted data follows after the encrypted data. This enables the possibility to encrypt very large fragmented messages. If N is set to 0000b, no encrypted data follows.

Security mode 7 requires a Configuration Field Extension according to Table 21.

Table 21 – Configuration Field Extension for security mode 7

MSBit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	LSBit 0
Reserved	Reserved for Version	KDF-Selection	KDF-Selection	KeyID	KeyID	KeyID	KeyID
0	0	D	D	K	K	K	K

K selects the KeyID for Encryption and Authentication used in the TPL. Applicable KeyID's are defined in 9.1 and 9.2.2.

D is 01b to mark key derivation function as defined in subclause 9.2.5.

A two-byte sequence 2Fh, 2Fh (decryption verification) shall immediately follow the Configuration Field Extension. The Decryption Verification Field is part of the Transport Layer.

7.2.4.5 Configuration Field for Security Mode 10

Security mode 10 is a symmetric authenticated-encryption method using AES128 with CCM and an ephemeral key (see 9.3.6). It is possible to identify up to 16 different communication security keys using the KeyID.

The Configuration Field (CF) to be used for security mode 0Ah is defined according to Table 22.

Table 22 – Configuration Field for security mode 10

MSBit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	LSBit 0
Content of Message	Content of Message	Counter Size	Mode 4	Mode 3	Mode 2	Mode 1	Mode 0	Number of encr. bytes	Number of encr. bytes	Number of encr. bytes	Number of encr. bytes	Number of encr. bytes	Number of encr. bytes	Number of encr. bytes	Number of encr. bytes
C	C	Z	M	M	M	M	M	N	N	N	N	N	N	N	N

M is always 0Ah to mark AES128 with CCM and ephemeral key.

C declares the Content of the Message (see 7.2.4.7).

Z is always 1b to declare that TPL contains a message counter (see 9.3.2) with a size of 4 bytes (acc. to [EN 13757-7:2018], 7.7.8).

N contains the number of encrypted bytes for CCM Mode. An N of 11111111b specifies that partial encryption is disabled and no unencrypted data follows after the encrypted data. This enables the possibility to encrypt very large fragmented messages. If N is set to 00000000b, no encrypted data follows.

Security mode 10 requires a Configuration Field Extension according to Table 23.

Table 23 – Configuration Field Extension for security mode 10

MSBit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	LSBit 0
Reserved	Reserved	Content Index	Content Index	Content Index	Content Index	Authentication Tag size	Authentication Tag size	Reserved	Version	KDF-selection	KDF-selection	KeyID	KeyID	KeyID	KeyID
0b	0b	I	I	I	I	O	O	0b	V	D	D	K	K	K	K

K selects the KeyID for the authenticated-encryption used in the TPL. Applicable KeyID's are defined in 9.1 and 9.2.2.

D is always 01b to mark key derivation function as defined in subclause 9.2.5.

NOTE 1: The Security Mode 10 applies only one derived key per direction, which is always the Kenc (DC=00h) for the authenticated encryption from the OMS end-device and Lenc (DC=10h) for the authenticated encryption from the gateway.

O is always 01b to mark an 8 byte Authentication Tag at the end of the message (acc. to [EN 13757-7:2018], 7.7.8).

If V is 1b then the field KeyVersion (KV) is present (1 byte, acc. to [EN 13757-7:2018], 7.7.8). Otherwise, V is 0b. OMS end-devices shall support an internal flag, called KI-Flag according to section 6.2.2. The V-flag of the Configuration Field Extension of mode 10 is set under the same conditions as this KI-flag. See section 6.2.2 for the rules for setting the KI-flag.

The use of KeyID, KeyVersion and Message counter for the TPL-security shall apply the corresponding fields from the TPL. If the AFL contains similar information, these AFL-fields shall be ignored.

I declares the Content Index of the Message (see 7.2.4.7)

NOTE 2: The Authentication Tag of the mode 10 is located in the TPL-Trailer of the Message after the APL. (see [EN 13757-7:2018], Table 20)

7.2.4.6 Configuration Field for Security Mode 13

Security mode 13 is an asymmetric encryption method using TLS (see Annex F).

Table 24 – Configuration Field for security mode 13

MSBit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	LSBit 0
Content of Message	Content of Message	Reserved	Mode 4	Mode 3	Mode 2	Mode 1	Mode 0	Number of encrypted bytes	Number of encrypted bytes	Number of encrypted bytes	Number of encrypted bytes	Number of encrypted bytes	Number of encrypted bytes	Number of encrypted bytes	Number of encrypted bytes
C	C	0	M	M	M	M	M	N	N	N	N	N	N	N	N

M is always 0Dh (13 decimal) to declare an Encryption with TLS

NOTE 1: The applied TLS-Version can be retrieved from the TLS-Header.

C declares the Content of message (see 7.2.4.7).

N contains the number of encrypted bytes. It indicates the number of bytes following the Configuration Field, which are covered by the Protocol indicated by Protocol type (TLS). N is limited to 255.

NOTE 2: For larger sizes the exact number of bytes (minus the TLS header size 5 Bytes) can be found in the 4th and 5th Byte of the TLS header.

Security mode 13 requires a Configuration Field Extension according to Table 25.

Table 25 – Configuration Field Extension for security mode 13

MSBit 23	Bit 22	Bit 21	Bit 20	Bit 19	Bit 18	Bit 17	Bit 16
Reserved	Reserved	Reserved	Reserved	Protocol Type 3	Protocol Type 2	Protocol Type 1	Protocol Type 0
0	0	0	0	P	P	P	P

P defines the Protocol Type (see Annex F).

NOTE 1: No Decryption Verification Field follows the Configuration Field.

NOTE 2: The usage of the mode 13 on wireless M-Bus requires the application of the Extended Link Layer.

7.2.4.7 Content of Message and Content Index

All security modes provide the bits CC in their Configuration Field that are used to describe the content of the message. They are defined in [EN 13757-7:2018], Table 21- Content of meter message and Table 22 – Content of partner message.

The identification of message contents is extended by the Content Index bits (IIII). Using those bits, a gateway is able to identify and store or filter messages with different content without the need to decrypt the application data. The following table shows the intended usage of the Content Index bits for an OMS end-device in relation to 8.4.4. Table 26 is valid for a content of message (CC = 00b) representing a standard data message.

NOTE 1: Content Index bits are only provided for Security Profile B and Security Profile D. Security profile B is supporting only the 3 least significant bits of the content index.

Table 26 – OMS usage of Content Index bits for CC = 00b

Content Index [IIII] (binary)	Contents of the message
0000	Legacy OMS end-device, no further usage of Content Index
0001	Data for mobile readout (MSO)
0010	Data for fixed network readout (MSO)
0011	Consumer information (CON)
0100 ... 0111	Manufacturer specific usage

Table 27 is valid for a content of message with CC = 01b representing an additional data message.

NOTE 2: A future issue of [EN 13757-7] will be enhanced with the CC = 01b value.

Table 27 – OMS usage of Content Index bits for CC = 01b

Content Index [IIII] (binary)	Contents of the message
0000 – 0011	Additional data for fixed network readout (MSO)
0100 – 0111	Reserved for future use
1000 – 1011	Additional data for fixed network readout (MSO)
1100 – 1111	Reserved for future use

NOTE 3: Other CC values might have a different interpretation of the IIII bits.

The expected content for each content index value is defined in 8.4.4. The relation between content index and message application is defined in 8.10.

7.2.4.8 Link Control Bits of the Configuration Field

The Configuration Field of security mode 5 and 0 supports the Link Control Bits B, A, S, R, and H. These bits may also be provided by lower layers.

If these bits do not exist in either ELL, LLC or MAC then

- the bit S shall be used as described in subclause 4.3.2.1
- bits B and A shall be used as described in subclause 4.3.3.1
- bits H and R shall be used as described in subclause 5.2.2.2.3.

Otherwise, these Link Control Bits in the Configuration Field should be set to zero.

If these bits exist in the lower layer, the Link Control Bits in the TPL shall be ignored (see 5.2.2.2.3).

The subclause 5.2.2.2.4 describes the conditions whether or not an Extended Link Layer exists in Mode C. For the usage of the Link Control Bits of OMS LPWAN see Annex Q.

7.3 Conditions to Apply the Transport Layer

The Transport Layer is required for message types with application data. Also message types without application data use the TPL to provide following services:

- OMS end-device address,
- Access number of the message,
- Reception level of the OMS end-device,
- Status byte (with result of the command execution from last SND-UD)

The OMS end-device shall apply the TPL for the message types according to Table 28.

Table 28 – Usage of TPL depending on message type

Direction	Message type	Presence TPL wired M-Bus	Presence TPL wireless M-Bus
Master to slave	SND-NKE	Never	Always
	SND-UD	Optional [a]	Always [b]
	SND-UD2	Optional [a]	Always
	REQ-UD1	Never	Always
	REQ-UD2	Never	Always [b]
	ACK	Not applicable	Always
	CNF-IR	Not applicable	Always
Slave to master	SND-NR	Not applicable	Always
	SND-IR	Not applicable	Always
	ACC-NR	Not applicable	Conditional [d]
	ACC-DMD	Not applicable	Always
	ACK	Never	Always [c]
	NACK	Not applicable	Never
	RSP-UD	Always	Always [b]

[a] In case of encryption the TPL is necessary
[b] For a fragmented message sequence the TPL shall only be in the first datagram (see 7.2.2.1)
[c] For a fragmented message sequence the TPL shall be at least in the last ACK (see 7.2.2.1 and L.4)
[d] If S-bit and ACC is not present in the lower layers (ELL or LLC), the TPL shall be provided (see 5.2.2.2.4).

8 Application Protocols

8.1 Overview

Possible Application Protocols for OMS end-device application data are:

- M-Bus (see 8.4)
- DLMS (see 8.5)
- SML (see 8.6)

Beside these Application Protocols for OMS end-device data exchange, some more Application Protocols for special services exist. These protocols are supported in case the conditions of Table 29 apply.

Table 29 – Application protocols

Name of Application Protocol [a]	Condition	Reference
Alarm	Support shall be declared in ManDec	[EN 13757-3:2018], Annex D
Application Error	Mandatory for bidirectional wireless or wired M-Bus	see 8.8
Application Select	Mandatory for bidirectional wireless or wired M-Bus	see 8.10
Clock Synchronisation	UC-04, Annex M	see 8.7
Image transfer	UC-05, Annex M	refer to [EN 13757-3:2018], Annex I
Network Management Protocol	Future UC, Annex M	Refer to [EN 13757-4:2019], clause 14
Security Information Transfer	Several use cases of Annex M; Security mode 13	Annex M, Annex F
Security Management Protocol	Security mode 13	see 8.9
[a] Refer to Table 1 column "Protocol or Service" for respecting CI-Field values		

8.2 Message Types and Their Application Data Content

8.2.1 Overview

The applicative content of a message from an OMS end-device depends on the message type and the current OMS end-device state. This state is influenced by internal and/or external events. This can e.g. be an internal transmission scheme, an external trigger, or a command.

There are following options to get application data from the OMS end-device

Table 30 – Message types and their application data content

Typical Application content	Trigger event	Message type	Reference
Installation data	Manually external trigger	SND-IR [a]	Clause 8.2.2
Consumption and management data	Periodically	SND-NR [a]	Clause 8.2.3
Alarm information	REQ-UD1	RSP-UD [b]	Clause 8.2.4
Any application data or command response	SND-UD[c]+REQ-UD2 or SND-UD2	RSP-UD	Clause 8.2.5

[a] Only for wireless M-Bus; wired M-Bus will provide this data with RSP-UD
[b] Alarm information can also be pushed by SND-NR
[c] SND-UD is optional and required for a command reply and application select

8.2.2 SND-IR

Figure 21 shows externally triggered push messages. Once the SND-IR message has been triggered, it is repeated several times.

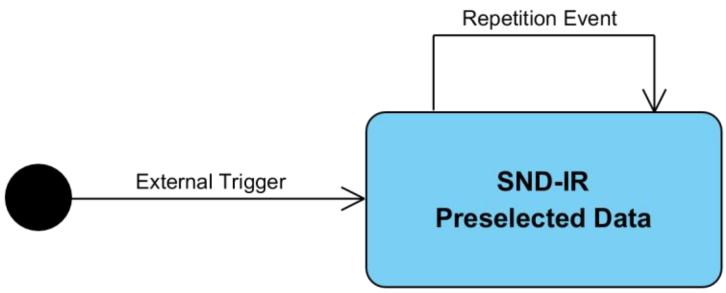


Figure 21 – States of an externally triggered transmission event

Table 31 – States of a SND-IR

State	Explanation	Reference
SND-IR Preselected Data	Provides preselected installation data according the rules for installation messages	Clause 4.3.2.4

Table 32 – State change events of a SND-IR

Event	Explanation	Reference
External trigger	An external trigger to start the installation mode, e.g. a push button	Clause 4.3.2.4
Repetition event	Installation messages are repeated several times	Clause 4.3.2.4

8.2.3 SND-NR/ACC-NR

For a SND-NR message there might be two different contents (dynamic and static). The dynamic data contains consumption data and other information, which may change frequently. The SND-NR with static data contains information for OMS end-device management that either never changes (e.g. id of metering point) or for which a rare update cycle is sufficient (e.g. changed ownership number). Between the SND-NR transmissions (dynamic or static), also ACC-NR messages without application data may be sent. There is no specific initial state. (see Figure 22)

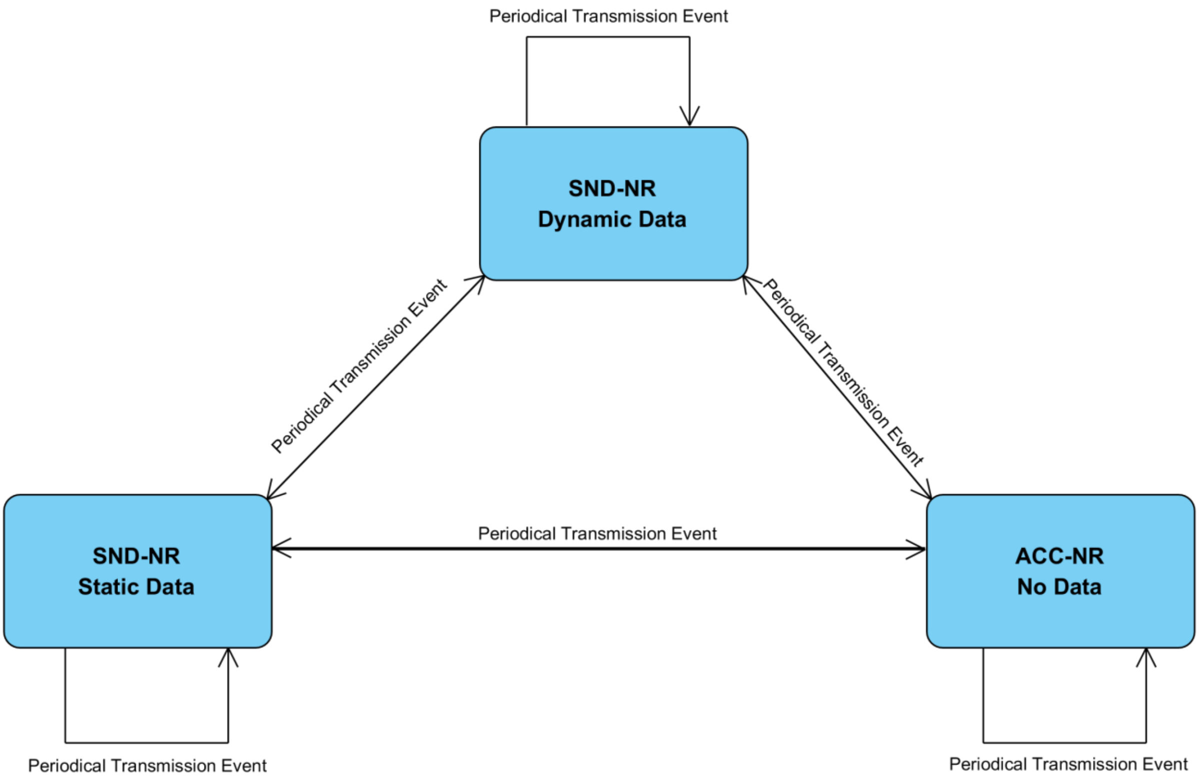


Figure 22 – States of a periodical transmission event

Table 33 – States of a SND-NR/ACC-NR

State	Explanation	Reference
SND-NR Dynamic Data	Provides consumption data according to an internal transmission scheme	Clause 4.3.2.2 Clause 8.4.4
SND-NR Static Data	Provides management data according to an internal transmission scheme	Clause 4.3.2.5
ACC-NR No Data	Provides only access to the OMS end-device according to an internal transmission scheme	Clause 4.3.2.1

Table 34 – State change events of a SND-NR/ACC-NR

Event	Explanation	Reference
Periodical transmission event	Transmission event according to a transmission scheme	Clause 4.3.2

8.2.4 RSP-UD/ACK after REQ-UD1

In case the OMS end-device supports the alarm protocol it can react with two different message types. Otherwise always an ACK shall be provided.

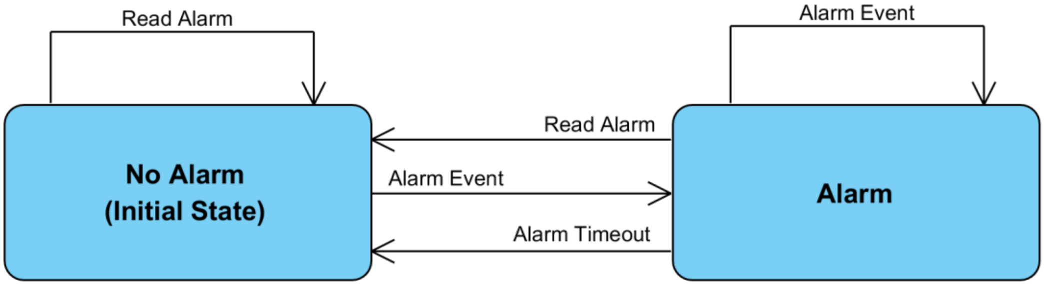


Figure 23 – Alarm response states

Table 35 – States of a RSP-UD/ACK after REQ-UD1

State	Explanation	Reference
No Alarm	In case of no alarm an ACK shall be sent	[EN 13757-4:2019] or [EN 13757-2:2018]
Alarm	In case of an alarm the alarm protocol should be sent	[EN 13757-3:2018] Annex D

Table 36 – State change events of a RSP-UD after REQ-UD1

Event	Explanation	Reference
Alarm Event	An internal event (manufacturer specific) that causes an alarm	
Read Alarm	With the transmission of the alarm by the RSP-UD message, the alarm should be cleared. [a]	[EN 13757-3:2018], Annex D
Alarm Timeout	A manufacturer specific timeout that clears the alarm	
[a] The message might stay in the sending buffer to provide repetitions according the transmissions rules, e.g. FAC		

8.2.5 RSP-UD after REQ-UD2 or SND-UD2

Figure 24 shows the applicative response states that define the content of a RSP-UD message after a REQ-UD2 or a SND-UD2. It also shows possible state change events. A REQ-UD2 itself is not a state change event whereas a SND-UD or SND-UD2 will influence the state according to the state change event table.

Specific data contents can be requested (e.g. with the Application Select Protocol see 8.10). Each command will react with dedicated applicative responses (see Annex B).

The initial state shall be automatically applied after the power-up, a device reset or after a disconnection from the wired M-Bus line as defined in [EN 13757-2:2018], 4.2.2.11.

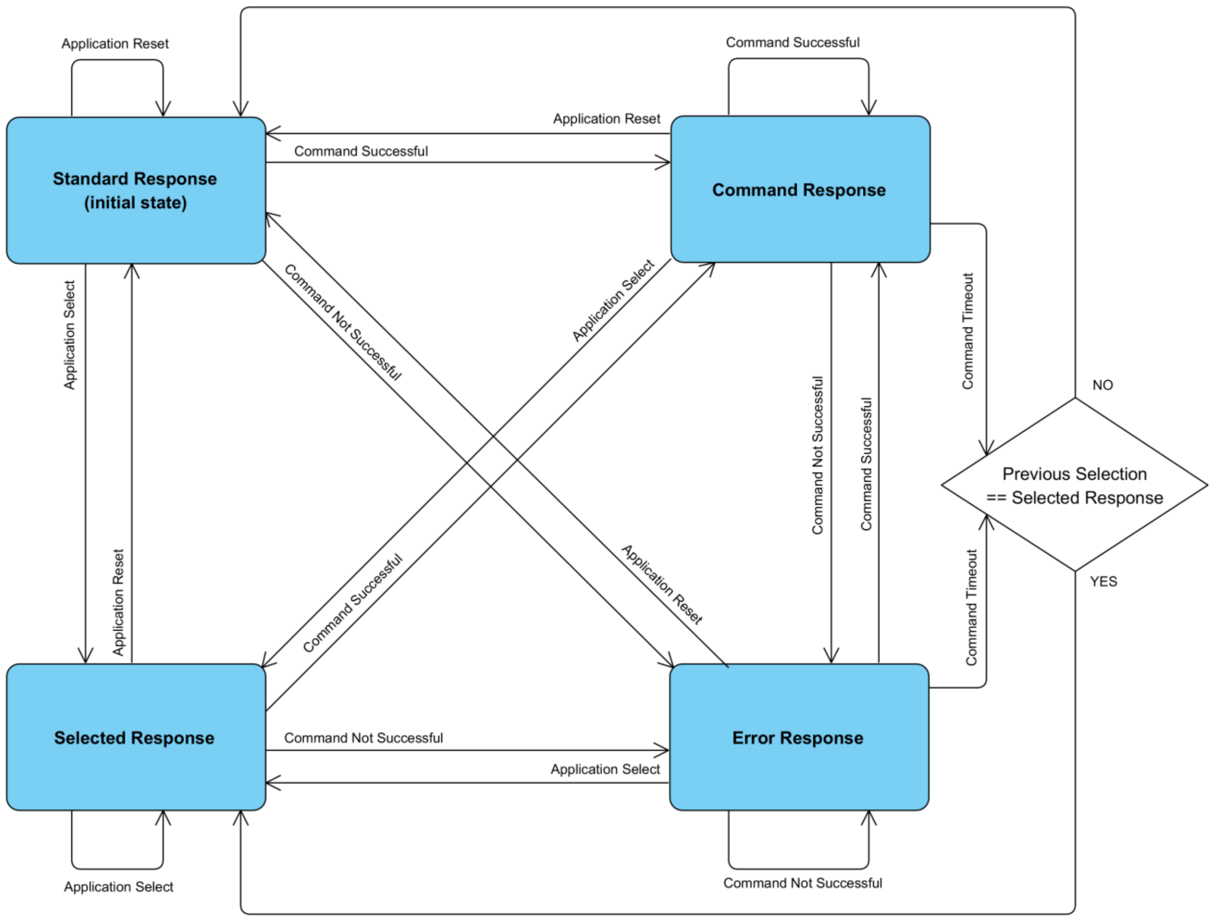


Figure 24 – Data response states

Table 37 – States of a RSP-UD after REQ-UD2/SND-UD2

State	Explanation	Reference
Standard Response	Defined by the manufacturer Contains mandatory data points	Clause 8.4.4
Selected Response	Contains data according chosen message application	Clause 8.10
Command Response	Applicative response to a command as defined in Annex M	Annex M
Error Response	Response to a command that caused an error e.g. with Application Error protocol	Clause 8.8 and [EN 13757-7:2018], Annex A.8.8

Table 38 – State change events of a RSP-UD after REQ-UD2/SND-UD2

Event	Explanation	Reference
Command Successful	Successfully received and processed command; recognisable by the indication of “no error” in the TPL status byte (see Table 17) of the corresponding response (ACK, RSP-UD).	Annex M
Command Not Successful	Successfully received but not successfully processed command; recognisable by the indication of “any application error” in the TPL status byte (see Table 17) of the corresponding response (ACK, RSP-UD).	Clause 8.8 and [EN 13757-7:2018], Annex A.8.8
Application Select	Selection of a dedicated message application	Clause 8.10
Application Reset	Selection of the standard response	Clause 8.10
Command Timeout	The timeout is 255 seconds and is started with the last command reception.	

8.3 Resolution and Accuracy of Consumption Data

An OMS end-device shall be in accordance with Annex C.2 of [CEN/TR 17167:2018].

If power or flow values are transmitted and the applied averaging interval is smaller than the nominal transmission interval, then the data point Averaging Duration should be transmitted additionally.

NOTE: The transmission of the Averaging Duration in the static datagram (see 4.3.2.5) will be sufficient.

8.4 M-Bus Application Protocol

8.4.1 General

The M-Bus Application Protocol is described in [EN 13757-3:2018]. To ensure interoperability, the use of the M-Bus Application Protocol in OMS is restricted by the following additional rules.

8.4.2 OMS-Data Point List

The Annex B lists all harmonised M-Bus-Data points in the OMS-Data point list (OMS-DPL). This list consists of a VIB-Type List and an M-Bus-Tag Lists.

The VIB-Type List provides all supported combinations of VIFs and VIFEs applied conforming to this specification.

The M-Bus tag lists provide all M-Bus tags applicable and conforming to this specification. An M-Bus-Tag is an abstract presentation of a single M-Bus data point or a set of M-Bus-Data points that differ by the scaler (see VIB-Type List of Annex B) or resolution.

8.4.3 OMS-Gateway

OMS-Gateways shall support all M-Bus data points listed in the OMS-DPL (see Annex B).

The standard load profile and the M-Bus compact profile according to [EN 13757-3:2018], Annex F shall be supported. See Annex G for examples for the conversion of load profiles to single data points.

M-Bus data points compliant with [EN 13757-3:2018], but not listed in the OMS-DPL, may optionally be supported by OMS-Gateways.

8.4.4 OMS end-device

OMS end-devices shall provide all M-Bus data points that are marked as mandatory (M) and at least one of the data points marked as alternative (Ax) in the OMS-DPL (see Annex B for the OMS end-device with the respective Device Type). Those data points are called “obligatory data points”. The exact DIB/VIB coding given in the Annex B shall be used. If multiple alternatives are provided in one message, all data points shall provide the required accuracy and resolution.

If the OMS end-device supports OMS use cases according to Annex M, it shall support the conditional data points as specified in Annex B.

Note that each data point shall be unique within a message. This means it is not allowed to provide the same combination of DIB (tariff, subunit, storage number, function code, final DIFE) and VIB in several data points. Several data points that differentiate only by the data type (INT/BCD), the measurement unit or the resolution are also not allowed.

Obligatory data points shall be present in the standard response (see 8.2.5).

NOTE: The standard response can be selected with an application reset [see [EN 13757-3:2018], clause 7].

Wireless devices shall additionally transmit obligatory data points with SND-NR messages according to Table 39. The obligatory data points shall be provided respecting the update interval maximum of Table 8.

Table 39 – Conditions for obligatory/conditional data points in SND-NR messages

Security Profile	Content of message [CC] (binary)	Content Index Field [IIII] (binary)	Synchronous / Asynchronous [S] (binary)	Are obligatory/ conditional data points required?	Origin of obligatory/ conditional data points
A, C	00	N/A	1	Yes	Annex B
B, D	00	0000 [a]	1	Yes	Annex B
A, C	00	N/A	0	No	N/A
B, D	00	0000 [a]	0	No	N/A
B, D	00	0001	0…1	No	N/A
B, D	00	0010	0…1	Yes	Annex B
B, D	00	0011	0…1	Yes	Annex M, UC-07
B, D	00	0100…0111 [b]	0…1	No	N/A
A, C	10	N/A	0…1	No	N/A
B, D	10	0000	0…1	No	N/A
B, D	01 [c]	0000 – 0011	0…1	No	N/A
D	01 [c]	1000 – 1011	0…1	No	N/A

[a] The combination of (CC = 00b; IIII = 0000b) shall only be transmitted by devices not supporting the differentiation of content according to Table 26 (backward compatibility).
[b] Use this to provide manufacturer specific content without providing obligatory data points.
[c] These combinations of Content of message and Content Indexes are used to provide additional data transmissions for fixed network readout.

If an OMS end-device provides additional M-Bus data points marked as optional (O) in the OMS-DPL, it shall use the exact DIB/VIB coding given there.

OMS end-devices may additionally use the standard load profile or the M-Bus compact profile according to [EN 13757-3:2018], Annex F. The underlying single M-Bus data points shall use the exact DIB/VIB coding given by the OMS-DPL. See Annex G for examples for the conversion of load profiles to single data points.

M-Bus data points that are listed in the OMS-DPL shall not be used in alternative or manufacturer specific sense.

Additional M-Bus data points that are not explicitly listed in the OMS-DPL, but comply with [EN 13757-3:2018], may optionally be provided by the OMS end-device. But these additional data points shall not be used as replacement for present data points in the OMS-DPL.

8.4.5 Usage of Specific Data Points

8.4.5.1 Date, Time and Intervals

For the averaging time interval of power or flow values the data point "averaging duration" (DP2!) shall be used (see 8.3).

For an uncorrelated transmission (refer to Annex C subclause C.2.3.2 in [CEN/TR 17167:2018] the elapsed time between measurement and transmission shall be coded with the data point "actuality duration" (DP1!).

The nominal transmission interval used for synchronous transmission should be declared in installation datagrams (if available) with the data point "period of nominal data transmissions" (in seconds or minutes, DP3!).

Any due date value (identified with storage number 1 and no final DIFE according to Annex B, e.g. VM1!D) shall be accompanied by the respective due date (DT2!D). In this case the due date shall either be provided in the same message than the due date value or in the static frame.

See also Annex G for rules of storage numbers in load profiles.

8.4.5.2 Management Data

Details about the error state indicated by status byte (see 7.2.3) shall either be coded with the data point "Error flags" (MM2!) or optionally with "Error flags (standard)" (MM3!).

If a sequence number is needed (to prevent the detection of zero consumption – refer to [EN 13757-7:2018], 7.5.5.2) it shall be coded as data point "Unique message identification" (ID6!).

For OMS end-device management the reception level of a received radio device can be transmitted with the data point "Reception or noise level" (refer to [EN 13757-3:2018], 6.4.4.1 Table 12 – Main VIFE code extension table, footnote d). This corresponds to M-Bus-Tag MM1!.

If this data point is used together with the Function field 10b in DIF, it declares that the quality limit of the reception level was exceeded by the received radio device. Example: 21h FDh 71h 9Ch marks a reception level > -100 dBm. This corresponds to M-Bus-Tag MM1!I.

If this data point is used together with the Function field 11b, it declares the typical noise level detected by this radio device. Example: 31h FDh 71h 9Fh means a noise level of -97 dBm. This corresponds to M-Bus-Tag MM1!E.

The applied DIN Address (see 3.2) of an OMS end-device can be provided in two data points. The original DIN Address supplied by the manufacturer is called "initial DIN Address" (ID7!). This address shall remain always unchanged and corresponds to the printed label. If an address element is subsequently changed by the operator, e.g. if a new device type is set, the new address can be given as "current DIN address" (ID8!).

8.4.5.3 Sensors

Sensors according to this specification shall apply either a device type listed in Table 9 or the device type1Fh together with a concerning sub device type (ID11!) according to [prEN13757:2023], 6.5]. See also timing requirements in 4.3.2.3.

8.4.6 OBIS Code

The Object Identification System (OBIS) defines the identification codes for commonly used data items in metering equipment.

These identification codes from DLMS-UA Blue Book are used for identification of:

- logical names of the instances of the interface classes, the objects
- data transmitted through communication lines
- data displayed on the metering equipment

OBIS-codes in addition are used for the market communication of different contract partners for the standardised exchange of metering values. M-Bus coded metering data needs a mapping to the relevant COSEM object instantiation with OBIS codes identifying the appropriate information. The Annex A defines a List of OBIS codes as subset of M-Bus-Tags from the OMS-DPL and the assigned OBIS codes. An OMS-Gateway that converts M-Bus data points to another Application Protocol shall add the respective OBIS code from the list.

If an OMS end-device uses an M-Bus data point that is not listed in the OMS-DPL, but is required for billing purposes, the OBIS declaration should be transmitted by the OMS end-device itself. A radio device should transmit this OBIS declaration by a static message (see 4.3.2.5). The OMS-Gateway then adds this OBIS declaration to the default OBIS conversion-table. The OBIS declaration via the M-Bus Application Protocol is described in [EN 13757-3:2018], Annex H.3.

8.4.7 Descriptors

M-Bus messages may contain several data points with the same VIB. They are separated using different Storage numbers, Tariff numbers, or Subunits (coded in the DIB). This allows the gateway to distinguish and group these data points e.g. using same Storage numbers. However, by default there is no information about the meaning of different storage, subunit or tariff numbers.

Data points listed in the Annex A can be interpreted by the assignment to the given OBIS-Code (e.g. HC1!D and DT2!D, coded with Storage number 1, are defined as value at due date). Other data points (e.g. coded with Storage number 2) provide no information about the meaning and their interpretation may vary between manufactures.

Descriptor data points (defined in Annex K) should be used to add a meaning to every data point group (e.g. all data points using Storage number 2 are used for monthly values). This enables the user to interpret the OMS end-device data points correctly. For some data points the usage of descriptors is mandatory (see Annex K).

In case a descriptor is required, a unidirectional OMS end-device shall send it in each data message that contains a data point that needs the descriptor, or in each static message (see 4.3.2.5). A bidirectional OMS end-device should send it in each data message that contains a data point that needs the descriptor, or in each static message. The gateway may also request descriptors from bidirectional OMS end-device using an Application select (see 8.10).

8.4.8 Commands

Further information on commands is given in Annex M.

8.5 DLMS Application Protocol

The DLMS Application Protocol for CEN meters is described in [EN 13757-1:2014], [EN 62056-6-1:2013] and [DLMS UA].

8.6 SML Application Protocol

The SML Application Protocol is described in document [SML-spec].

8.7 Clock Synchronisation Protocol

If the gateway or the AMMHES provides the clock management service (according to Annex M, OMS-UC-04), the clock synchronisation protocol shall be applied. This protocol (time setting, time adjustment) is defined in the [prEN 13757-3:2023], Annex E.3. This annex defines criteria for periodical adjustments and adjustments on events. These criteria are not mandatory for OMS. Instead, the clock accuracy and the adjustment interval is in the responsibility of the gateway respectively AMMHES operator.

NOTE: The synchronisation of the OMS end-device clock may be in conflict with national laws. Check Annex E for details.

8.8 Application Error Protocol

When an OMS end-device detects a failure in terms of authentication check, decryption, interpretation, or execution of a received command, it shall generate an application error. The presence of an application error should be announced in the Status field (see Table 17). Details of the application error may be requested by the gateway with a REQ-UD2. The application error shall remain until a respective state change event takes place (see Table 38).

The application error shall be transmitted with the generic Application Error Protocol as defined in [EN 13757-3:2018], clause 10 (see also Table 1 in 2.2).

Table 40 lists application error codes that are harmonized by OMS. Other error codes of [EN 13757-3:2018], 10.3, Table 21 – “First error code byte for general application errors” are also allowed.

Table 40 – OMS Application error codes

Error code	Designation	Description	Application example
01_h	CI-Field error	Unimplemented CI-Field	SITP not supported
03_h	Record overflow	Too many records	Too many M-Bus tags added (see Annex M, UC-14)
08_h	Application busy	Application too busy for handling readout request	If a REQ-UD2 arrives before the application response has been generated
10_h	Command not yet finished	The command is currently being processed and cannot be started again.	Second clock adjustment command while first one is still in process (see OMS-UC-04).
11_h	No function	Function not implemented (command unknown or not supported)	If an unknown DIF/VIF-combination was received.
12_h	Data error	Data to be supplied are not available	If the access to the data source fails e.g. connection between adapter and OMS end-device broke.
15_h	Parameter error	Parameter is missing or wrong	Clock adjustment command which exceed defined limit (see OMS-UC-04).
17_h	Message structure error	Expected fields or communication layers are not present or invalid in the message.	Missing AFL or missing AFL.MAC
20_h	Security error	Message counter check, decryption or authentication fails or selected key is not available	Wrong AFL.MAC
21_h	Security mechanism not supported	Security mode in the AFL/TPL in a SND-UD or SND-UD2 is not supported.	A SND-UD with security mode 8 was received.
22_h	Inadequate security method	Security method or key is not applicable for this function	A secured function like “Clear status information” was transmitted without SITP.

Application errors shall be transmitted unencrypted and not authenticated (see Table 42) as long as they are not wrapped in an application security protocol (see 9.4).

NOTE 1: The Application Error Protocol can only be used for bidirectional communication.

NOTE 2: An erroneous application select does not cause an application error (see 8.10).

8.9 Security Management Protocol

The Security Management Protocol provides services to establish and manage session based secured data transfer channels like TLS. It is initiated with specific CI-Fields (see Table 1). After a successful establishment the application data (e.g. M-Bus coded metering data initiated with CI = 72h) can be transferred within this secured channel.

The structure of the security management data depends on the security mode defined in the TPL Configuration Field and other security mode specific fields in the Configuration Field/ Configuration Field Extension. The first implementation of the Security Management Protocol is defined for the security mode 13 (see 9.3.8), which is needed for the OMS Security profile C using Transport Layer Security (TLS). Details are described in Annex F.

8.10 Application Select Protocol

The Application Select Protocol is used to request selected data from a bidirectional OMS end-device (according to [EN 13757-3:2018], clause 7). Table 41 shows the harmonized message applications and their relation to the fields content of message and content index. The application reset or select with CI-fields according to Table 1 acts as permanent application selection. If an application select is used without any parameter, then it acts as an application reset. An application reset forces the fall-back to the standard response (see [EN 13757-3:2018], clause 7).

The application can also be selected with command setMM6!. Such a command applies a temporarily application select only (see Annex M, UC-14). The concerning command response is MM6!. Both the command and the response shall use a coding according to [EN 13757-3:2018], 7.2.

The content of the static message (see 4.3.2.5) can also be reached with an application select to subcode 7 (see [EN 13757-3:2018], 7.2, Table 19 – Coding of the message application). If the static message contains descriptors (see 8.4.7) they shall either be in block 0 or in block 1.

If the OMS end-device does not support the selected application it shall apply an application reset according to [EN 13757-3:2018], 7.4.2.

If the OMS end-device cannot provide the selected block number it shall select the first block of the selected application according to [EN 13757-3:2018], 7.5.

Table 41 – List of message applications

Message application	Related content of message CC (acc. to 7.2.4.7)	Related content index (acc. to 7.2.4.7)	Description
07	10b	0000b	Static content
16	00b	0001b	Data for mobile readout
17	00b	0010b	Data for fixed network readout
18	00b	0011b	Data for consumer information (acc. to Annex M, UC-07)
26	00b	0100b	Manufacturer specific usage
27	00b	0101b	Manufacturer specific usage
28	00b	0110b	Manufacturer specific usage
29	00b	0111b	Manufacturer specific usage
46	01b	0000b	Add. data for fixed network readout
47	01b	0001b	Add. data for fixed network readout
48	01b	0010b	Add. data for fixed network readout
49	01b	0011b	Add. data for fixed network readout
54	01b	1000b	Add. data for fixed network readout
55	01b	1001b	Add. data for fixed network readout
56	01b	1010b	Add. data for fixed network readout
57	01b	1011b	Add. data for fixed network readout

9 Security

9.1 General

The Open Metering System provide security mechanism for the

- Communication security (see 9.3) to protect the link between the OMS end-device and the communication partner and
- Application security (see 9.4) to protect and authorise application services

Sub-clause 9.2 defines the rules for the applicable keys.

To protect the privacy of the consumer, all wireless communication containing consumption data shall be encrypted (according to 9.3). For wired communication, the encryption/authentication is optional (according to 9.3).

However, if encryption for the communication channel is enabled not all messages need to be encrypted. Table 42 lists for each protocol / layer whether or not the encryption/authentication is required, possible, or not allowed, in case of enabled security profile. Messages without a transport layer are generally not encrypted.

Even if encryption for an application protocol is required, some data points like Identification or Fabrication number need to be transmitted unencrypted. Annex B.2 lists for each M-Bus data point whether or not the encryption (according to 9.3) is required, possible, or not allowed.

Annex F lists requirements for encryption/authentication of TLS-handshake messages.

Annex E lists additional national requirements.

Table 42 – Encryption and authentication of application protocols

CI-Field	Protocol / Layer	Encryption	Authentication
50h [a]	Application Reset or Select	N/A	Off
51h [a]	Command (M-Bus)	N/A	Off
52h	Selection of Device	N/A	Off
53h, 57h [e]	Application Reset or Select	🔒	On
54h [a]	Request of selected application	N/A	Off
55h, 56h [e]	Request of selected application	🔒	On
5Ah, 5Bh [g]	Command (M-Bus)	🔒	On
5Fh [f]	Command (TLS-HS)	see Annex F	see Annex F
60h, 61h [b, f]	Command (DLMS)	🔒	On
64h, 65h [b, f]	Command (SML)	🔒	On
66h [a]	Response of selected application	N/A	Off
67h, 68h [e]	Response of selected application	🔒	On
6Ch, 6Dh, 62h	Time Sync	🔒	On
6Eh, 6Fh [c, h]	Application Error	🔓	Off

Table 42 (continued)

CI-Field	Protocol / Layer	Encryption	Authentication
70h	Application Error	N/A	Off
71h	Alarm	N/A	Off
74h, 75h	Alarm	🔒 [e]	On
		🔓	Off
72h, 7Ah [g]	Response (M-Bus)	🔒 see Annex B.2 [d]	On
7Ch, 7Dh [b, f]	Response (DLMS)	🔒	On
7Eh, 7Fh [b, f]	Response (SML)	🔒	On
80h, 8Ah, 8Bh, 93h	Pure Transport Layer	🔓	Off
9Eh, 9Fh [f]	Response (TLS-HS)	see Annex F	see Annex F
B8h	Set baud rate to 300 baud	N/A	Off
BBh	Set baud rate to 2400 baud	N/A	Off
BDh	Set baud rate to 9600 baud	N/A	Off
BEh	Set baud rate to 19200 baud	N/A	Off
BFh	Set baud rate to 38400 baud	N/A	Off
C0h, C1h, C2h, C7h [e]	Image transfer	🔒	On
C3h, C4h, C5h, C6h [e, h]	Security Information Transfer	🔒	On

🔒 Encryption is mandatory. A Security mode > 0 shall be applied.
🔓 Encryption is not allowed. Security mode 0 shall be applied.
N/A Not applicable

[a] These CI-Fields are not applicable, if the communication requires a Security profile (see Table 44).
[b] These commands/responses encrypt and authenticate data using either the security services of AFL/TPL (according to this specification) or APL specific security methods.
[c] For Security profile C the encrypted transmission of application errors is allowed. For details see Annex F.
[d] Not all data points need to be encrypted. The size of encrypted data may vary from zero to full data length.
[e] In case data need to be padded before encryption, TPL-padding acc. to [EN 13757-7:2018], 9.4.5.4 shall be used.
[f] TPL-padding acc. to [EN 13757-7:2018], 9.4.5.4 is optional.
[g] In case data need to be padded before encryption, padding value 2Fh in the application protocol shall be used.
[h] Application protocol wrapped in SITP will use TPL encryption and authentication according to Annex M.2

NOTE 1: Column “authentication” shall be ignored if a security profile is applied, that does not support authentication, e.g. Security Profile A.

NOTE 2: If no encryption and no authentication is required, Security mode 0 (see 9.3.4) can be used.

The usage of a MAC (see 9.3.3) ensures the integrity and the authenticity of the transferred data.

A persistent key is usually configured to an OED by an operator action and has a long validity time. It can be used for encryption, authentication, or key derivation. For some cipher methods a key is derived from the persistent key. Such a key is called ephemeral key and is used for encryption or authentication. It has a short validity time or is used only once.

Table 43 provides an overview of the supported security profiles. Each profile presents a valid combination of the encryption method, message authentication, and the length and type of used key.

Table 43 – OMS Security profiles

Profile	Encryption	Authentication	Key
No Security profile	No encryption (Security Mode 0) [a]	No MAC (MAC-Mode AT = 0) [b]	No key
Security profile A [g]	AES128-CBC (Security Mode 5) [a, d,]	No MAC (MAC-Mode AT = 0) [b, d]	128 bit persistent symmetric key (with KeyID acc. to 9.2.2)
Security profile B	AES128-CBC (Security Mode 7) [a, d]	CMAC (8 Byte trunc.) (MAC-Mode AT = 5) [d, e]	128 bit ephemeral symmetric key (derived by KDF from persistent key with KeyID acc. to 9.2.2)
Security profile C	TLS 1.2 (Security Mode 13) [a, d]	HMAC (TLS1.2) and additional CMAC (8 Byte trunc.) (MAC-Mode AT = 5) [d, e] for communication establishment	256 bit elliptic curve key (384 bit optional) for TLS and 128 bit ephemeral symmetric key (derived by KDF from persistent key with KeyID acc. to 9.2.2) for CMAC [c]
Security profile D	AES128-CCM (Security Mode 10) [a, d]	CCM (8 Byte) (OO=01b) [d, f]	128 bit ephemeral symmetric key (derived by KDF from persistent key with KeyID acc. to 9.2.2)

[a] Declared in Configuration Field CF (see 7.2.4)
[b] If AFL is not present the default interpretation is AT = 0.
[c] During the TLS-handshake the usage of the CMAC is also required. However, the normal data exchange of Mode 13 applies the HMAC of the TLS protocol for message authentication.
[d] The following message types shall apply Security mode 0 and no AFL: REQ-UD1, REQ_UD2, SND-NKE, ACC-NR, ACC-DMD, ACK, NACK, CNF-IR
[e] Declared in AFL.MCL (see [EN 13757-7:2018]).
[f] Declared in CFE of security mode 10 (see 7.2.4.5)
[g] The security profile A will be deprecated and is not recommended by OMS for future development.

Table 44 defines which Security profiles shall be supported by the OMS end-device and the gateway.

Table 44 – Required Security profiles

Communication	OMS end-device	OMS-Gateway
Wireless, unidirectional communication (according to 4.3)	Security profile A or Security profile B or Security profile D	Security profile A and Security profile B and Security profile D
Wireless, bidirectional communication (according to 4.3) [a]	Security profile A or Security profile B or Security profile C or Security profile D	Security profile A and Security profile B and Security profile D and optionally Security profile C
Wired communication (according to 4.2)	No security profile or Security profile A or Security profile B or Security profile D or Security profile C	No security profile and Security profile A and Security profile B and Security profile D and optionally Security profile C
[a] In addition to the security profiles listed here, "no security profile" may be used by LPWAN communications, as far as the LPWAN communication provides similar security services as shown in Table 43.		

The manufacturer shall declare all supported security profiles in the data sheet of an OMS end-device or gateway. During operation the OMS end-device is not allowed to change the configured security profile by itself. The security profile can only be changed with an OMS end-device configuration procedure initiated e.g. by the MSO.

NOTE: The asymmetric encryption (e.g. Security profile C) of bidirectional communication is necessary for certain countries due to national laws. It can provide a higher security level for transmissions where AES-based encryption with shared keys is not sufficient. Annex E provides a guideline to solutions which meet the known national requirements.

9.2 Key Management

9.2.1 General

An OMS end-device has one or several keys. If an OMS end-device provides access for different users or if it has different communication end points (like gateway or AMMHES) then different keys have to be used. Keys with different purpose can be identified by the KeyID (see 9.2.2). A key used for replacement of an existing key, applies the same KeyID but a different KeyVersion (see [EN 13757-7:2018]). An OMS end-device has at least the master key MK.

9.2.2 KeyID

Each key is defined for one specific purpose. The KeyID is used to identify the key and its usage. Table 45 lists available KeyID. Changing one key shall not have any effect on keys with other KeyID.

Table 45 – Predefined OMS-KeyIDs

Techno-logy	Key-ID (Hex)	Usage	Responsible
Symmetric	00h	Master key (MK), default communication security key	OMS-Group
	01h to 07h	Manufacturer specific communication security key	Manufacturer
	08h	Harmonised communication security key (see Annex M, OMS-UC-07b)	OMS-Group
	09h to 0Eh	Reserved for harmonised communication security keys	OMS-Group
	0Fh	MAC key, persistent key for OMS LPWAN MAC security (see Annex Q)	OMS-Group
	10h	Root wrapper key applicable to wrapper keys with a KeyID 10h to 16h; (see Figure 25 and Annex M; OMS-UC-08)	OMS-Group
	11h	Reserved for wrapper keys	OMS-Group
	12h	Communication security wrapper key; applicable to communication security keys with KeyID 00h and 08h to 0Fh; optional applicable to KeyID 01h to 07h (see Figure 25 and Annex M, OMS-UC-08)	OMS-Group
	13h	Reserved for wrapper keys	OMS-Group
	14h	Application security wrapper key; applicable to APL keys with a KeyID 18h to 2Fh (see Figure 25 and Annex M, OMS-UC-08)	OMS-Group
	15h	Reserved for wrapper keys	OMS-Group
	16h	Reserved	OMS-Group
	17h	Manufacturer specific wrapper key	Manufacturer
	18h	Authentication key for firmware image protection (See Annex M, OMS-UC-05)	OMS-Group
	19h to 1Eh	Reserved	OMS-Group
	1Fh	Application security key for OMS compliance test (See Annex M, OMS-UC-00)	OMS-Group
	20h	Application security key for disconnection & reconnection (See Annex M, OMS-UC-03)	OMS-Group
	21h	Application security key for clock adjustment (See Annex M, OMS-UC-04b/-04c)	OMS-Group
	22h	Application security key for clock setting (See Annex M, OMS-UC-04b/-04c)	OMS-Group
	23h	Application security key for update of firmware image (See Annex M, OMS-UC-05)	OMS-Group
	24h	Application security key for OMS end-device supervision (See Annex M, OMS-UC-06)	OMS-Group
	25h	Application security key for data selection (See Annex M, OMS-UC-14)	OMS-Group
	26h	Application security key for application management (See Annex M, OMS-UC-12)	OMS-Group
	27h	Application security key for settings of an adapter (See Annex M, OMS-UC-20)	OMS-Group
	28h to 2Fh	Reserved for harmonised APL-Keys	OMS-Group
	30h to 4Fh	Manufacturer specific APL-Keys	Manufacturer
	50h to 5Fh	Reserved for harmonised APL-Keys	OMS-Group
	60h to 7Fh	Reserved	-

Table 45 – Predefined OMS-KeyID (cont.)

Techno-logy	Key-ID (Hex)	Usage	Responsible
Asymmetric	80h to AFh	Defined in Annex F	OMS-Group
	B0h to BFh	Reserved for harmonized Keys	OMS-Group
	C0h to EFh	Manufacturer specific Keys	Manufacturer
	F0h to FFh	Reserved	-

NOTE: Communication security keys used for security services in TPL and AFL can apply only KeyID-numbers from 00h to 0Fh.

9.2.3 Key Generation

The master key (KeyID = 0) shall be generated by a cryptographic random generator.

The master key shall be generated for each device individually.

The communication security key with KeyID = 8 shall apply to the same rules as the master key.

NOTE: Possible references for random generators are [BSI_TR-02102-1] or [NIST_800-133].

9.2.4 Key Exchange

The OMS end-device may have several keys. Each key is used for a special purpose and can be identified by the KeyID (see 9.2.2). The key exchange uses the Security information protocol according to [EN 13757-7:2018], Annex A. Details for the exchange of symmetric keys are defined in Annex M, OMS-UC-08.

Symmetric and asymmetric keys used for Security profile C require a specific key exchange procedure as defined in Annex F.

The key exchange requires so called wrapper keys, which are used to wrap the new key in a secured container before the key is transferred to the OMS end-device. There is a wrapper key for the communication security keys used in the AFL/TPL and another wrapper key for the application security keys used in the APL. The wrapper keys themselves can be exchanged only by the root wrapper key. The root wrapper key itself is also exchangeable by the root wrapper key. The root wrapper key shall not be used to exchange other keys than wrapper keys. Following figure illustrates the key hierarchy.

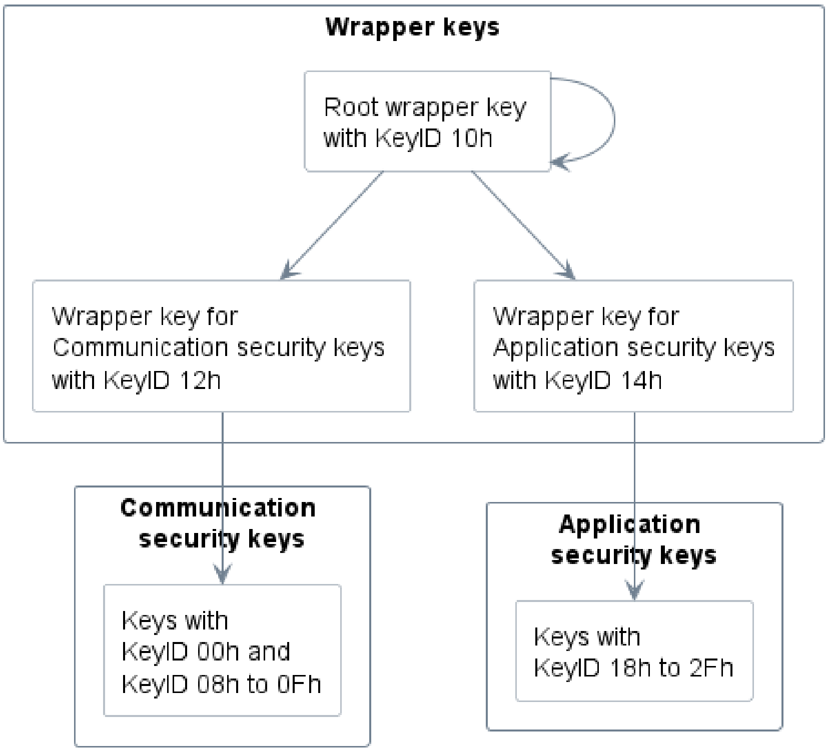


Figure 25 – Keys used for the key exchange of symmetrical keys.

The root wrapper key is the security basis for all other keys. The owner of this key has the possibility to change all other keys. Therefore, it shall never be forwarded to other parties. The owners of other keys (wrapper keys, communication security keys) can recognize an (unwanted) interference by the root wrapper key with help of the key version of the respective key (increased key version number in that case).

9.2.5 Key Derivation Function

9.2.5.1 General

If an ephemeral key is required then the key shall be generated using the key derivation function defined below. This ephemeral key shall be used for one message only. The key derivation function shall apply the CMAC function according to [RFC4493]. There are five input values to the KDF specified in 9.2.5.2 to 9.2.5.6.

9.2.5.2 Communication Security Key (CSK)

Before each transmission up to two ephemeral keys, Kenc (for encryption) and Kmac (for authentication), are derived from the individual communication security key CSK. There are two sets of key pairs (one set for the OMS end-device Kenc/Kmac and one set for the gateway Lenc/Lmac).

If nothing else is defined the master key (MK) shall be used as communication security key (CSK).

The initial master key MK_0 (provided by the manufacturer) has the KeyID = 0 and the KeyVersion = 0. If the OMS end-device provides Security Profile C according to Annex E.1 this initial master key MK_0 shall be stored permanently and shall not be removed or replaced when the operator provides a new master key. A new master key will get the same KeyID but a different KeyVersion. The initial master key MK_0 is linked to a dedicated initial message counter C_{M0} (see 9.3.2.3).

9.2.5.3 Derivation Constant (DC)

The constant is used to derive different keys for both Encryption and Authentication as well as for the two directions - from and to the OMS end-device.

Table 46 – Constant (DC) for the key derivation

DC	Used for
00h	Encryption from the OMS end-device (Kenc)
01h	MAC from the OMS end-device (Kmac)
10h	Encryption from the gateway (Lenc)
11h	MAC from the gateway (Lmac)

9.2.5.4 Message counter

The KDF applies the message counter to generate a unique ephemeral key for each new message. The message counter shall be according to 9.3.2.

9.2.5.5 Device ID

The device ID used in the key derivation function corresponds to the Identification Number of the OMS end-device address.

The location of this address in uplink and downlink messages is defined in 3.1.

9.2.5.6 Padding

To avoid the generation of the K2 (refer to [RFC4493]) in the KDF, the remaining bytes of the 16 byte block are filled with a padding sequence. For the generation of Kmac, Lmac and Kenc, Lenc the padding is fixed and consists of seven octets each containing the value of 07h according to the rule that the input to the MAC shall be padded with (16-l mod 16) bytes with value (16-l mod 16), where l equals the byte length of the input.

9.2.5.7 Key calculation

The calculation of encryption and authentication key:

```
K = CMAC( CSK , DC || C || ID || 07h || 07h || 07h || 07h || 07h ||
              07h || 07h )
```

Where

- CSK is individual communication security key (according to 9.2.5.2)
- DC is Derivation constant (according to 9.2.5.3)
- C is message counter C_M, C'_M, C''_M, C_{GW} or C'_{GW} (according to 9.2.5.4)
- ID is Device ID (according to 9.2.5.5)

Multi byte fields C and ID are arranged in the same order as in the transmitted frame.

The derived key K can be Kenc, Kmac, Lenc, Lmac depending on selected Derivation constant (see 9.2.5.3).

Figure 26 in 9.3.2.2 and Figure 27 in 9.3.2.4 provides a detailed sequence diagram for transmitting and receiving messages using a derived key.

9.3 Communication security

9.3.1 General

Communication security protects the communication between the OMS end-device and the communication partner like the gateway. It covers protection of privacy and integrity. It also prevents a zero-consumption detection. The encryption applies only to the application protocol and the decryption verification and TPL-padding (if present).

In case of several communication partners, the OMS end-device has to maintain an individual message counter for each applied communication security key.

The security mode in use is indicated in the Configuration Field (see 7.2.4).

9.3.2 Message counter

9.3.2.1 Overview

Ephemeral keys are generated by inclusion of a strictly monotonously increasing (non-secret) counter in the KDF. This counter is transmitted either in the AFL.MCR field for security profile B and C (see [EN 13757-7:2018], 6.3.5) or in the TPL for security profile D (see [EN 13757-7:2018], 7.7.8). The message counter maintained and transmitted by the OMS end-device is named C_M, the message counter maintained and transmitted by the communication partner (typically the gateway) is named C_{GW}.

A copy of this message counter stored by the receiver of the message is marked as C' respectively C''.

The following set of counters is needed for data exchange:

- C_M counter used by the OMS end-device as message counter;
- C_{GW} counter used by the communication partner as message counter;
- C'_{GW} unverified copy of C_{GW} used by the OMS end-device;
- C'_M unverified copy of C_M used by the communication partner;
- C''_M verified copy of C_M used by the communication partner;

The OMS end-device counter C_M is the leading counter in the system.

NOTE: The message counter is required for Security profile B, C and D (see 9.1)!

An example for the handling of the message counter is provided in Annex J.

9.3.2.2 Message counter handling in an OMS end-device

C_M is used for the derivation of keys applicable to messages transmitted from the OMS end-device to the communication partner.

The initial value of C_M is 0. The OMS end-device shall increment C_M by 1 prior to generating an authenticated and encrypted message.

C_M shall be updated, if an authenticated and valid message counter C_{GW} from a communication partner was received as shown in Figure 26.

When the counter C_M reaches the maximum value FFFFFFFFh it shall not wrap around with the next increment. In this case the OMS end-device should stop any transmission.

In case the individual master key (KeyID K = 0) of the OMS end-device is changed, the counter C_M shall be reset to the initial value.

Figure 26 shows the handling of the message counter in an OMS end-device for both transmitting and receiving a message.

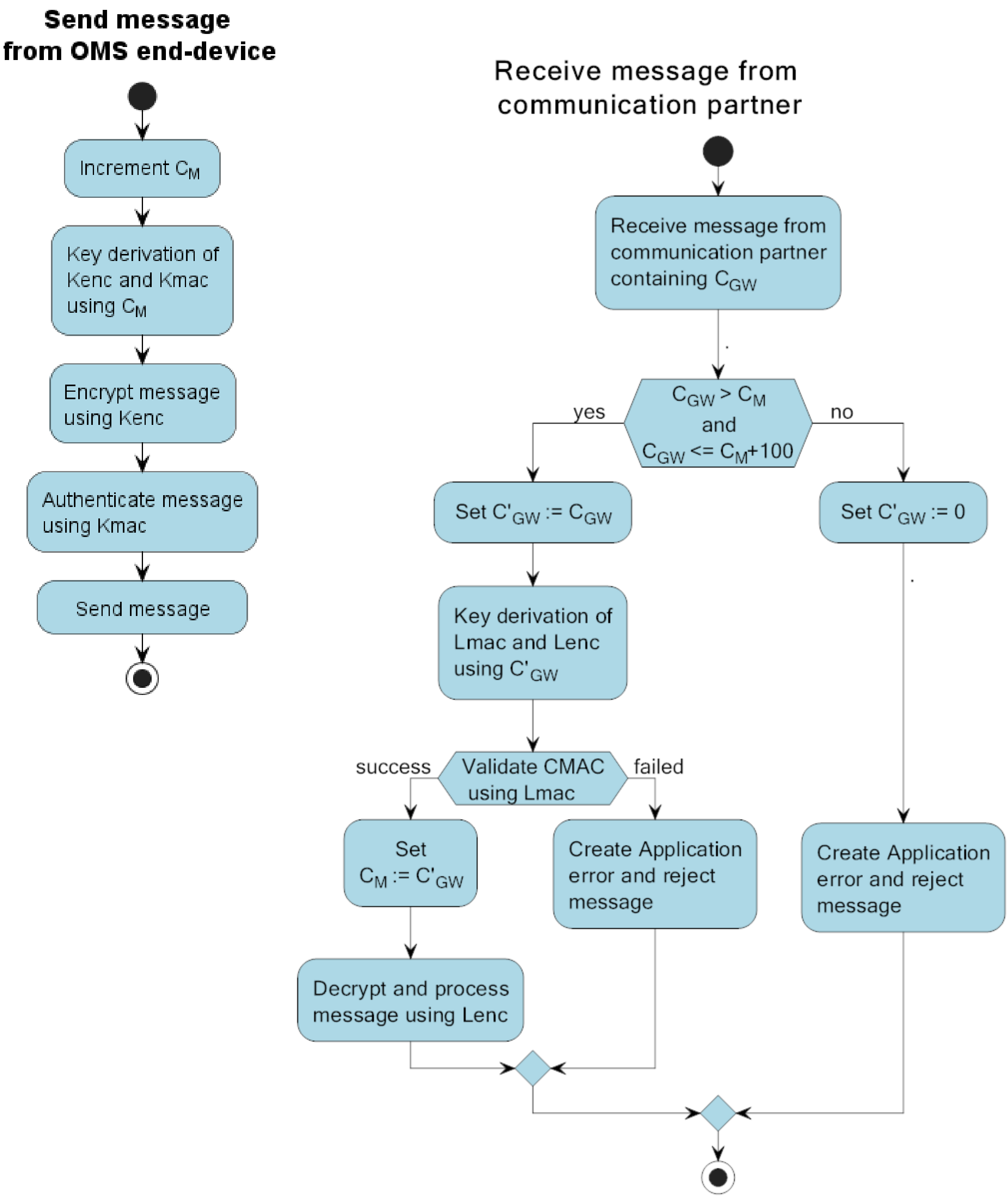


Figure 26 – Handing of the message counter in the OMS end-device

9.3.2.3 Initial Message Counter C_{M0}

If an OMS end-device provides Security Profile C according to Annex F, it has to maintain an additional message counter called initial message counter C_{M0}. This specific message counter is only linked to the initial master key MK_0 (see 9.2.5.2). The initial value of C_{M0} is 0. It shall only be increased, if the initial master key MK_0 is active. A reset of the initial message counter is never possible. The last value of the initial message counter must always be stored (and proceeded) for a later communication with the initial master key in case of a "Reset of MK_0".

The message counter C_M shall not be influenced by the initial message counter C_{M0}. If a new master key is used, the message counter C_M will be reset. The initial message counter C_{M0} is not harmed by this process.

9.3.2.4 Message Counter Handling in a Communication Partner

C_{GW} is used for the derivation of keys applicable to messages transmitted from the communication partner to the OMS end-device.

NOTE: The communication partner supports an independent message counter C_{GW} for each connected OMS end-device.

The initial value of C_{GW} for each OMS end-device is 0.

C_{GW} shall be updated, if an authenticated message counter C_M from OMS end-device was received as shown in Figure 27.

The communication partner shall increment C_{GW} prior to generating an authenticated and encrypted message. The increment shall not exceed the value of 100.

When the counter C_{GW} reaches the maximum value FFFFFFFFh it shall not wrap around with next increment. In this case the communication partner should stop any transmission to this OMS end-device.

When the communication partner receives a message counter C_M ≥FFFF0000h it should set the OMS end-device in error condition to trigger a service action (e.g. master key exchange) before the message counter of the OMS end-device reaches the maximum value.

Figure 27 shows the handling of the message counter in a communication partner for both transmitting and receiving a message.

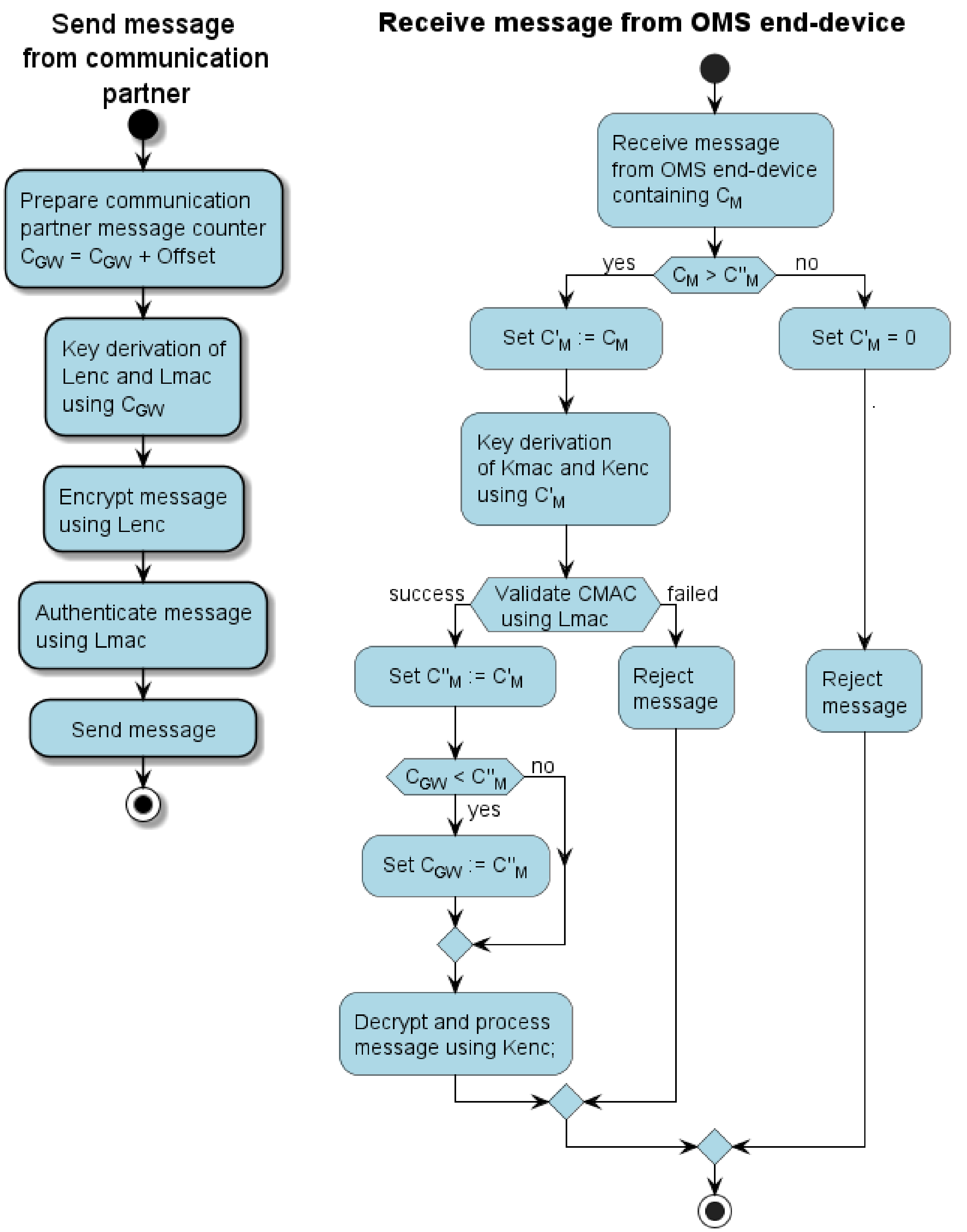


Figure 27 – Handing of the message counter in the communication partner

NOTE: Because of the short time window for replying to a wireless M-Bus datagram, a communication partner may calculate the encryption key and authentication key in advance, based on the assumption of a message counter value (C_M'').

9.3.3 MAC-Generation

9.3.3.1 CMAC (AES 128 – 8 Byte Truncated)

The authentication of the message is supported by the AFL (option AT = 5 – see [EN 13757-7:2018]) using the MAC. This MAC shall be calculated as specified in AES128 for Crypto-Message-Authentication (CMAC-AES128) according to [RFC4493]. The MAC shall be calculated as follows:

```
MAC = CMAC (Kmac/Lmac, AFL.MCL || AFL.MCR[7..0] || AFL.MCR[15..8] ||
AFL.MCR[23..16] || AFL.MCR[31..24] || { AFL.ML[7..0] ||
AFL.ML[15..8] || } NextCI || ... || Last Byte of message)
AFL.MAC = trunc(MAC)
```

The presence of the AFL.ML field depends on the selection bits in the AFL.MCL field.

The MAC shall be calculated after the encryption. The MAC of a received message shall be verified before decryption.

An example is given in Annex N.

For a transmission from communication partner to OMS end-device the key Lmac is used. For a transmission from OMS end-device to communication partner the key Kmac is used (see key calculation in subclause 9.2.5.7).

The resulting 16 byte of this CMAC-function shall be truncated to 8 bytes as defined in [RFC4493]. Thus, the first 8 bytes beginning with the MSB shall be taken in the field AFL.MAC.

In deviation to the usual transmission order for octet strings on the M-Bus, the MSB of the MAC shall be transmitted as first byte, the LSB as last.

9.3.3.2 HMAC (TLS1.2)

The TLS1.2 requires a HMAC for the authentication of the payload. TLS message authentication is part of the TLS protocol. See Annex F for details.

9.3.4 No Encryption with Security Mode 0

If security mode 0 is selected, then all following data are transmitted plain.

9.3.5 Symmetric Encryption with Security Mode 5

Symmetric encryption is performed with security mode 5. It uses AES-CBC with a persistent key of 128 bits and a specific dynamic initialisation vector based on the Access Number of the Transport Layer. The initialisation vector requires the usage of the Access Number. Be aware that the initialisation vector shall always apply the Access Number from the Transport Layer whether or not the Extended Link Layer exists. The security mode is defined in [EN 13757-7:2018], 9.4.4.

The data to be encrypted shall be padded to a multiple of 16 bytes before encryption. The padding method depends on the selected application protocol (refer to Table 42).

Annex N shows examples with both unencrypted and encrypted data.

9.3.6 Symmetric Encryption with Security Mode 7

Symmetric encryption is performed with security mode 7. It uses AES-CBC with an ephemeral key of 128 bits and a static initialisation vector IV = 0 (16 Bytes of 00h). The security mode is defined in [EN 13757-7:2018], 9.4.5.

The ephemeral key shall be generated with a key derivation function (KDF), which is described in subclause 9.2.5.

For ensuring the integrity and authenticity, the CMAC as described in subclause 9.3.3.1 shall be used.

Applying the security mode 7 always requires the usage of the AFL (see clause 6), since the message counter C (see 9.2.5.4) is needed for the KDF and transmitted in the AFL.

The data to be encrypted shall be padded to a multiple of 16 bytes before encryption. The padding method depends on the selected application protocol (refer to Table 42).

Annex N shows examples with both unencrypted and encrypted data.

9.3.7 Symmetric Authenticated-Encryption with Security Mode 10

Symmetric authenticated-encryption is performed with security mode 10. It uses AES-CCM with an ephemeral key of 128 bits. The security mode is defined in [EN 13757-7:2018], 9.4.8.

The ephemeral key shall be generated with a key derivation function (KDF), which is described in subclause 9.2.5. Applying the security mode 10 does not require the usage of the AFL, since the message counter MC (see 9.2.5.4) needed for the KDF is transmitted in the TPL of security mode 10 and since the authentication is provided with an authentication tag in the TPL of security mode 10.

The CCM of security mode 10 ensures integrity and authenticity by including an 8 byte authentication tag. The authentication tag is further providing decryption verification.

The data to be encrypted does not need to be padded before encryption.

Refer to Annex D for further information on the TPL-structure of security mode 10.

9.3.8 Asymmetric Encryption with Security Mode 13

Security Mode 13 describes an asymmetric encryption method based on Transport Layer Security (TLS). Security mode 13 is defined in Annex F.

NOTE: It should be noted that the TLS (Transport Layer Security) according to Security profile C is independent from the KDF and CMAC. Nevertheless, the CMAC is required for the TLS-handshake procedure to protect it against DoS attacks[6].

9.4 Application security

9.4.1 General

The communication security (according to 9.3) is used to protect the link between the communication partner and the OMS end-device. Critical functions may be separately protected, to avoid unintended or unauthorised actions by users with access to the metering system. The application security provides the service of an additional security level in the application layer.

The application security is not an alternative to the communication security but has to be applied additionally for critical functions. Following figure illustrates the different access rights of User1 and User2 provided by the application security.

[6] A denial-of-service (DoS) attack is an attempt to make a service unavailable to its intended users.

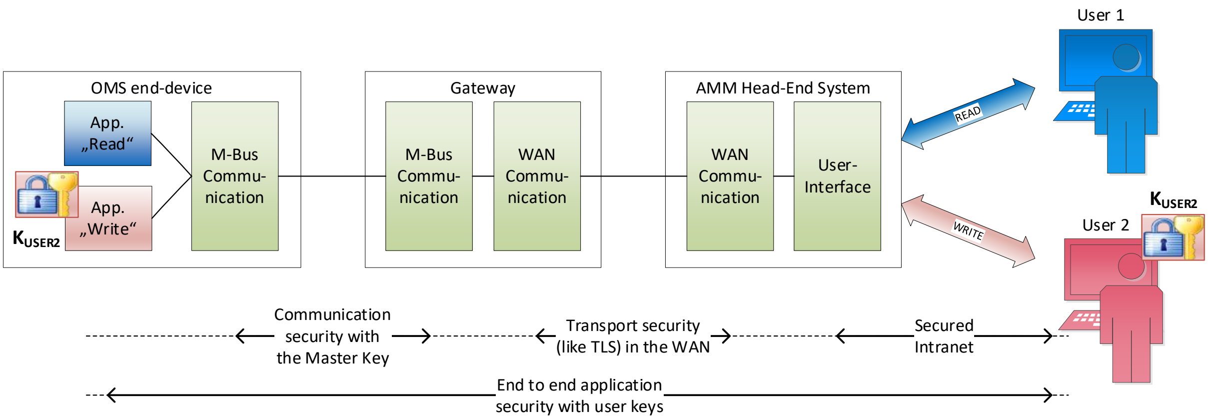


Figure 28 – Application security versus Communication security

To protect critical services of an OMS end-device against unauthorised usage, the critical application command or response are encapsulated in a specific secured protocol. This protocol is called Security Information Transfer Protocol (SITP). The SITP is defined in [prEN 13757-7:2023], Annex A.

The usage of the SITP is required

- To support selected use cases (described in Annex M) and
- To allow key exchange in Security profile C.

NOTE: Typically, the commands to be secured by application security are enciphered in the AMM Head-End System, whereas the communication or transport security is applied in the communication partner. For this reason, it is essential that the application security applies different keying material than the communication security.

9.4.2 Application security profile

9.4.2.1 Overview

Table 47 describes the Application security profiles that may be supported by an OMS end-device. The mandatory or optional use of Application security profiles are defined in Annex M.

Table 47 – OMS Application security profiles

Profile No	Application	Cipher method	According to:
ASP01	Key Exchange (symmetrical keys only)	Key wrap based on AES128	[prEN 13757-7:2023], Annex A, A.8
ASP02	Exchange of security information for Security profile C	Key wrap based on AES128 + ASN.1 DER	Annex F, appendix F.A
ASP03	Authentication of a firmware image	CMAC (16 Byte) based on AES128	[prEN 13757-3:2023], Annex I, I.2.4.6 (MAC Algorithm ID 04h)
ASP04 to ASP09	Reserved		
ASP10	End to end authenticated application data	CMAC (8 Byte) based on AES128	[prEN 13757-7:2023], Annex A, A.9.4 (DSI 32_h)
ASP11 to ASP19	Reserved		
ASP20 [a]	End to end secured application data	AES-CCM (8 Byte) based on AES128	[prEN 13757-7:2023], Annex A, A.9.7 (DSI 36_h)
[a] This ASP is intended for use cases that need additional confidentiality.			

Each Application security profile shall be used together with a special KeyID. The applicable KeyID’s are described in 9.2.2.

All keys applied for application security are 128 bit persistent symmetric keys.

9.4.2.2 ASP01 - Key Exchange

This Application security profile is used together with use case “Key management” (see Annex M, OMS-UC-08). It allows a secured exchange of symmetrical keys (see 9.2.4) in the OMS end-device.

9.4.2.3 ASP02 - Exchange of Security Information for Security Profile C

The SITP is also used for the exchange of security information of Security profile C. Because this Security profile applies an asymmetrical crypto mechanism the SITP-protocol has been extended. The Annex F defines the extension of SITP.

9.4.2.4 ASP03 – Authentication of a Firmware Image

This Application security profile is only used together with the use case “Firmware update” (see Annex M, OMS-UC-05). It provides an Authentication of the transferred firmware image.

9.4.2.5 ASP10 - End to End Authenticated Application Data

This profile allows transferring application data in an authenticated SITP container. The OMS end-device shall only accept messages, if the verification of the authentication has been passed.

The transported application protocol is identified by the Protocol Identifier field (PID). The Annex M lists the applicable PIDs for each use case.

9.4.2.6 ASP20 - End to End Secured Application Data

This profile allows transferring application data in a secured (confidential and authenticated) SITP container. The OMS end-device shall only accept messages, if the verification of the security has been passed.

The transported application protocol is identified by the Protocol Identifier field (PID). The PID is same link in 9.4.2.5.

Annex

Annex A (Normative): List of OBIS Codes for OMS end-devices

The list of OBIS codes provides a translation between an M-Bus-Tag and a relevant COSEM object instantiation with OBIS code identifying the appropriate information. This list is applicable when the M-Bus-data points are converted to another protocol.

This annex may be subject to a more frequent update than this main document. Therefore, the annex is not included. The current version (Release F or later) can be downloaded from the OMS website (www.oms-group.org).

Annex B (Normative): OMS-Data Point List

This annex provides a list of all M-Bus-Tags supported by the OMS.

This annex may be subject to a more frequent update than this main document. Therefore, the annex is not included. The current version (release G or later) can be downloaded from the OMS website (www.oms-group.org).

Annex C (Empty)

This annex is intentionally left blank.

NOTE: This annex has been used until OMS-S2, v 4.5.1. With the revision of sensors in [prEN 13757-3:2023] and [prEN 13757-7:2023] all necessary definitions for sensors are inside this document.

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

The TPL/APL (starting from the TPL-CI-Field) uses one of the following frame structures.

NOTE: These structures show only fields used by OMS. According to [EN 13757-7:2018] more fields may occur before and after the application data.

D.1 No TPL-header

The No TPL-header may be used on wired M-Bus. The application protocol starts immediately after the CI-Field.

TPL/APL without TPL-header

No message identification by Access Number, Status or encryption possible.

- Applied from master with CI = 50h; 51h; 52h; 54h
- Applied from slave with CI = 66h; 70h; 71h

CI	Data

TPL without TPL-header

No message identification by Access Number, Status or encryption possible.

- Applied from master with CI = B8h … BFh

CI

D.2 Short TPL-header

The Short TPL-header can be applied if the OMS end-device application address is identical with the link address of the wireless M-Bus OMS end-device. On wired M-Bus, the Short TPL-header is applicable in downlink only.

TPL/APL with Short TPL-header

- Applied from master with CI = 56h, 57h, 5Ah; 61h; 62h, 65h, 92h, C6h, C7h
- Applied from slave with CI = 67h; 6Eh; 74h; 7Ah; 7Dh; 7Fh; 88h, 9Eh, C1h, C4h

CI	ACC	STS	CF/ CFE	(KV)	(MC)	(DV)	Data	(AT)

NOTE: The fields in brackets exists only in case of special security modes (see D.4).

TPL with Short TPL-header

- Applied from master with 93h
- Applied from slave with CI = 8Ah

CI	ACC	STS	CF/ CFE

D.3 Long TPL-header

If the OMS end-device application address differs from the link address of the wireless M-Bus OMS end-device or if a wired M-Bus OMS end-device is used, then the Long TPL-header with support of mandatory Secondary Address shall be applied.

TPL/APL with Long TPL-header

- Applied from master with CI = 53h, 55h, 5Bh; 5Fh; 60h; 64h; 6Ch, 6Dh, C0h, C3h
- Applied from slave with CI = 68h; 6Fh; 72h; 75h; 7Ch; 7Eh; 9Fh, C2h, C5h

CI	Ident. No	Manuf.	Ver.	Dev. Type.	ACC	STS	CF/ CFE	(KV)	(MC)	(DV)	Data	(AT)

NOTE: The fields in brackets exists only in case of special security modes (see D.4).

TPL with Long TPL-header

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

CI	Ident. No	Manuf.	Ver.	Dev. Type	ACC	STS	CF/ CFE

D.4 Legend

CI	Control Information Field
Ident. no	Identification Number (part of OMS end-device application address)
Manuf.	Manufacturer ID (part of OMS end-device application address)
Ver.	Version (part of OMS end-device application address)
Dev. Type	Device Type (part of OMS end-device application address)
ACC	Access Number (from master initiated session uses Gateway Access Number; from slave initiated session uses Meter Access Number)
STS	Status (from master to slave) used for gateway status (RSSI); (from slave to master) used for OMS end-device status
CF/ CFE	Configuration Field / Configuration Field Extension
(KV)	KeyVersion (only present in security mode 10 and only if enabled in the CF/CFE)
(MC)	Message counter (only present in security mode 10)
(DV)	Decryption Verification – a two-byte sequence 2Fh 2Fh (only present in security mode 5 and 7)
(AT)	Authentication Tag located in the TPL-Trailer (only present in security mode 10).
Data	Application data; coding depends on used Application or Service Protocol

Annex E (Normative): Communication profiles for compliance with national regulations

A national law may require additional demands on the security of OMS end-device communication. This annex lists the applicable communication profiles in order to comply with the national regulation.

Annex E may be subject to a more frequent update than this main document. Therefore, the annex is not included. The current version (Release A or later) can be downloaded from the OMS website (www.oms-group.org).

E.1 Requirements for Smart Meter Gateways in Germany

The German law requires an approval for the operation of a Smart Meter Gateway in Germany. This approval checks both the security and the interoperability of a Smart Meter Gateway. The [BSI TR03109] describes the requirement to such a Smart Meter Gateway.

Such a Smart Meter Gateway has to reject an unsecure communication link to a smart OMS end-device. The Annex E.1 describes which services and security methods of the OMS-Specification shall be applied and which services are not allowed to conform to [BSI TR03109].

E.2 Requirements for Compliance with IDIS Association in Europe

This section describes the functionalities and features that an OMS end-device must support in order to be able to communicate with an IDIS E-meter according to IDIS Pack 3.

Annex F (Normative): Transport Layer Security (TLS) with Wireless M-Bus

The German law requires an approval for the operation of a Smart Meter Gateway in Germany. This approval checks both the security and the interoperability of a Smart Meter Gateway. The [BSI TR03109] describes the requirements to the interface of a Smart Meter Gateway.

One requirement is the TLS-protection of connections to meters with a bidirectional communication interface in the Local Metrological Network (LMN). This annex describes a BSI conform implementation of a TLS-communication on the wireless M-Bus.

TLS protected communication may also be used on wired M-Bus connections. However, the wired M-Bus interface is not a mandatory interface of a Smart Meter Gateway according to [BSI TR03109].

Annex F may be subject to a more frequent update than this main document. Therefore, the annex is not included. The current version (Release B or later) can be downloaded from the OMS website (www.oms-group.org).

Annex G (Normative): Conversion of a Load Profile to Single Data Points

G.1 Treatment of Historical Values in Compact Load Profiles with Registers

Sets of historical billing values, indicated by the value group F (with F<255) of an OBIS-Code and assigned to dedicated COSEM objects, are always coded with a final DIFE with the value 00h. The number of DIFEs is variable. Such sets of historical billing values shall use a Compact Load Profiles with registers.

The final DIFE shall be used in the DIBs of all three related data points (Base Time, Base Value and Compact Load Profile with registers).

NOTE: Sets of historical billing values, indicated by the value group F (with F = 255) of an OBIS-Code, like a Due Date Value, never use the final DIFE and apply the Compact Load Profile without registers.

G.2 Applicable Standard

The Standard load profile and the Compact Load Profile shall be compatible to the description of [EN 13757-3:2018], Annex F.

The orthogonal VIFE of the Compact Load Profile, as defined [EN 13757-3:2018], Annex F, F.2.6 to F.2.8, shall be used as last VIFE in the VIB.

NOTE: If an MB tag from Annex B is to be used as a compact profile, set the extension bit (see [EN 13757-3:2018], 6.3.6) of the last VIF/VIFE and append the corresponding orthogonal VIFE.

G.3 Applicable Storage numbers

For the OMS Conformance test a standard profile or a compact profile will be first converted to a set of single data points (see G.3 to G.6) before the compliance with Annex B is checked. For these single data points, the transmitted storage number and the following storage numbers are used. All these storage numbers shall not overlap with the storage numbers of other transmitted data points having a different reference time.

G.4 Data Set of the Example

The following examples show how an original set of periodical consumption values is coded as Standard Load Profile or Compact Load Profile and how these Load Profiles are converted to a set of single M-Bus data points.

Table G.1 – Example: Load profile of consumption values for a water meter

1st value at the end of the month	2008-01-31	65 litres (10^{-3} m³)
2nd value at the end of the month	2008-02-29	209 litres
3rd value at the end of the month	2008-03-31	423 litres
4th value at the end of the month	2008-04-30	755 litres
Last value at the end of the month	2008-05-31	1013 litres

G.5 Example for Standard Load Profile

Table G.2 – Example: Standard Load Profile composed of the periodical volume values

DIB		VIB	Data	Hex coded (LSB first)
Data field	**Storage number**			
2 digit BCD	8	Size of storage block	5	89 04 FD 22 05
2 digit BCD	8	Storage interval in months	1	89 04 FD 28 01
16 bit binary	12	Date (Type G)	2008-05-31	82 06 6C 1F 15
8 digit BCD	8	Volume (liters)	65	8C 04 13 65 00 00 00
8 digit BCD	9	Volume (liters)	209	CC 04 13 09 02 00 00
8 digit BCD	10	Volume (liters)	423	8C 05 13 23 04 00 00
8 digit BCD	11	Volume (liters)	755	CC 05 13 55 07 00 00
8 digit BCD	12	Volume (liters)	1013	8C 06 13 13 10 00 00

Table G.3 – Example: Periodical volume values converted to single data points

DIB		VIB	Data	Hex coded (LSB first)
Data field	**Storage number**			
16 bit binary	8	Date (Type G)	2008-01-31	82 04 6C 1F 11
8 digit BCD	8	Volume (liters)	65	8C 04 13 65 00 00 00
16 bit binary	9	Date (Type G)	2008-02-29	C2 04 6C 1D 12
8 digit BCD	9	Volume (liters)	209	CC 04 13 09 02 00 00
16 bit binary	10	Date (Type G)	2008-03-31	82 05 6C 1F 13
8 digit BCD	10	Volume (liters)	423	8C 05 13 23 04 00 00
16 bit binary	11	Date (Type G)	2008-04-30	C2 05 6C 1E 14
8 digit BCD	11	Volume (liters)	755	CC 05 13 55 07 00 00
16 bit binary	12	Date (Type G)	2008-05-31	82 06 6C 1F 15
8 digit BCD	12	Volume (liters)	1013	8C 06 13 13 10 00 00

NOTE: Corresponding table cells in Tables *G2* and *G3* are marked with corresponding background colours.

G.6 Example for Compact Load Profile

Table G.4 – Example: Compact Load Profile composed of the periodical volume values

DIB		VIB	Data						Hex coded LSB first
				Spacing control byte					
Data field	Storage number		LVAR	Increment mode	Spacing unit	Data field	Spacing value byte	Data	
8 digit BCD	8	Volume (liters)						65	`8C 04 13 65 00 00 00`
16 bit binary	8	Format G						2008-01-31	`82 04 6C 1F 11`
Variable length	8	Volume (liters)	10	Incre-ments	Full month	4 digit BCD	254	144, 214, 332, 258	`8D 04 93 1F 0A 7A FE 44 01 14 02 32 03 58 02`

Table G.5 – Example: Periodical volume values converted to single data points

DIB		VIB	Data	Hex coded (LSB first)
Data field	Storage number			
16 bit binary	8	Format G	2008-01-31	`82 04 6C 1F 11`
16 bit binary	9	Format G	2008-02-29	`C2 04 6C 1D 12`
16 bit binary	10	Format G	2008-03-31	`82 05 6C 1F 13`
16 bit binary	11	Format G	2008-04-30	`C2 05 6C 1E 14`
16 bit binary	12	Format G	2008-05-31	`82 06 6C 1F 15`
8 digit BCD	8	Volume (liters)	65	`8C 04 13 65 00 00 00`
8 digit BCD	9	Volume (liters)	209	`CC 04 13 09 02 00 00`
8 digit BCD	10	Volume (liters)	423	`8C 05 13 23 04 00 00`
8 digit BCD	11	Volume (liters)	755	`CC 05 13 55 07 00 00`
8 digit BCD	12	Volume (liters)	1013	`8C 06 13 13 10 00 00`

NOTE: Corresponding table cells in Tables *G4* and *G5* are marked with corresponding background colours.

G.7 Example for an Inverse Compact Load Profile

Table G.6 – Example: Inverse Compact Load Profile composed of the periodical volume values

DIB		VIB	Data						Hex coded LSB first
Data field	Storage number		LVAR	Spacing control byte			Spacing value byte	Data	
				Increment mode	Spacing unit	Data field			
8 digit BCD	8	Volume (liters)						1013	`8C 04 13 13 10 00 00`
16 bit binary	8	Format G						2008-05-31	`82 04 6C 1F 15`
Variable length	8	Volume (liters)	10	Incre-ments	Full month	4 digit BCD	254	258, 332, 214, 144,	`8D 04 93 13 0A 7A FE 58 02 32 03 14 02 44 01`

Table G.7 – Example: Periodical volume values converted to single data points

DIB		VIB	Data	Hex coded (LSB first)
Data field	Storage number			
16 bit binary	12	Format G	2008-01-31	`82 04 6C 1F 11`
16 bit binary	11	Format G	2008-02-29	`C2 04 6C 1D 12`
16 bit binary	10	Format G	2008-03-31	`82 05 6C 1F 13`
16 bit binary	9	Format G	2008-04-30	`C2 05 6C 1E 14`
16 bit binary	8	Format G	2008-05-31	`82 06 6C 1F 15`
8 digit BCD	12	Volume (liters)	65	`8C 04 13 65 00 00 00`
8 digit BCD	11	Volume (liters)	209	`CC 04 13 09 02 00 00`
8 digit BCD	10	Volume (liters)	423	`8C 05 13 23 04 00 00`
8 digit BCD	9	Volume (liters)	755	`CC 05 13 55 07 00 00`
8 digit BCD	8	Volume (liters)	1013	`8C 06 13 13 10 00 00`

NOTE: Corresponding table cells in Table G.6 and Table G.7 are marked with corresponding background colours.

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

H.1 Glossary

Table H.1 – Glossary of the Gas meter consumption data

V_m	The volume at measurement conditions
V_{tc}	Temperature converted volume
V_b	The volume at base conditions
Measurement conditions	Conditions of the gas whose volume is measured at the point of measurement (e.g. the temperature and the pressure of the gas) [EN 12405]
Base conditions	Fixed conditions used to express the volume of gas independently of the measurement conditions [EN 12405]
Converted volume	The converted volume from the quantity measured at measurement conditions into a quantity at base conditions

H.2 Overview

For billing purposes, the measured volume of a gas meter needs to be converted into energy. Depending on the technology of the gas meter there might be several parameters for this conversion:

- Temperature
- Pressure
- Gas calorific value

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

In general, the mentioned conversions can be done explicitly using devices measuring, the specific condition, or also implicitly by meters that measure independently from the specific condition.

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

H.3 Volume at Measurement Conditions

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

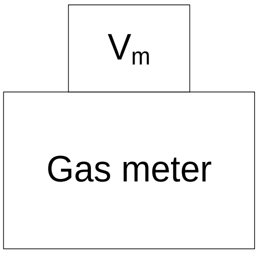


Figure H.1 – Gas meter providing volume at measurement conditions

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

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

H.4 Temperature Converted Volume V_{tc}

An individual meter based volume conversion to V_{tc} (in contrast to the “global” billing centre based conversion) can be achieved either mechanically or electronically. It can be implemented either internally in the meter or by some external conversion device, which then transmits converted values to the billing centre. Note that such a temperature conversion is based on a base temperature, which must be known to the billing centre. The default value for such a temperature at base conditions is 15 °C according to the [EN 1359].

If a meter uses a different base temperature, its temperature at base conditions information shall be transmitted with each volume data message.

Note that meter data can be converted by the billing centre to its “billing temperature at base conditions”, if this is different either from the default temperature of 15 °C or from the meters transmitted temperature at base conditions.

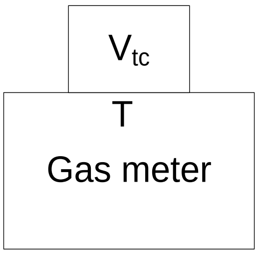


Figure H.2 – Gas meter providing temperature converted volume

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

H.5 Temperature and Pressure Converted Volume

In addition to a volume conversion just regarding temperature, an individual meter might convert its measured volume to base conditions regarding temperature and pressure. To comply with standard conditions, which are usually stated by national regulations and to allow the creation of gas bills that can easily be understood by the consumer, the same temperature at base conditions shall be used as for the calorific value in the case when both temperature and pressure are converted.

Devices complying with this do not need to send the information of the temperature at base conditions.

Note that a purely pressure converted volume, without temperature, is not supported.

Such a volume conversion is based on a pressure at base conditions, which must be known to the billing centre. The default value for such a pressure at base conditions is 1013,25 mbar. If a meter uses a different value for pressure at base conditions, such pressure at base conditions information shall be added to each volume data message.

Note that meter data can be converted at the billing centre to its “billing pressure at base conditions”, if this is different either from the default pressure of 1013,25 mbar or from the meter’s transmitted pressure at base conditions.

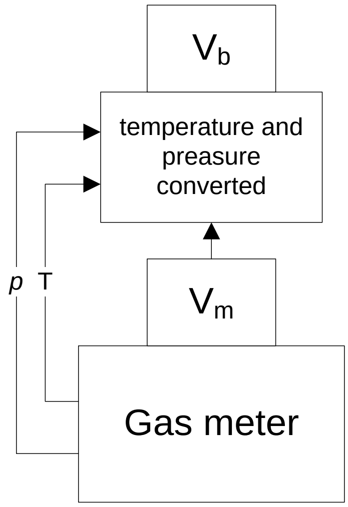


Figure H.3 – Gas meter providing temperature and pressure converted volume

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

H.6 OBIS / COSEM Application of Physical Units for Gas

(Extract from [DLMS UA] Blue Book ed. 13)

Table H. shows available physical units for the gas data objects given above. By application of a scale factor (ref. Table H3) the values can be scaled as required.

Table H.2 – Enumerated values for physical units

Unit ::= enum	Unit	Quantity	Unit name	SI definition (comment)
(9)	°C	temperature (*T*)	degree-Celsius	K – 273,15
(13)	m^3	volume (*V*) r_V , meter constant or pulse value (volume)	cubic meter	m^3
(14)	m^3	Converted volume	cubic meter	m^3
(19)	l	Volume	litre	10^{-3} m^3
(23)	Pa	pressure (*p*)	pascal	N/m^2
(24)	bar	pressure (*p*)	bar	10^5 N/m^2
(52)	K	temperature (*T*)	kelvin	

Some examples are shown in Table H.3 below.

Table H.3 – Examples for scaler-unit

Value	Scaler	Unit	Data
263788	-3	m^3	263,788 m^3
593	3	Wh	593 kWh
3467	0	V	3467 V

Annex I (Normative): Collision Avoiding Mechanism of the Gateway

The following describes a mechanism for automatic retransmissions from interrogating devices in order to resolve collisions on the radio channel. The algorithm is based on a maximum number of N retries (with N = 11) and choosing a random listen-after-talk-timeslot of the addressed OMS end-device. Furthermore, it evaluates the received message types to prevent disturbing other conversations.

I.1 Flowchart

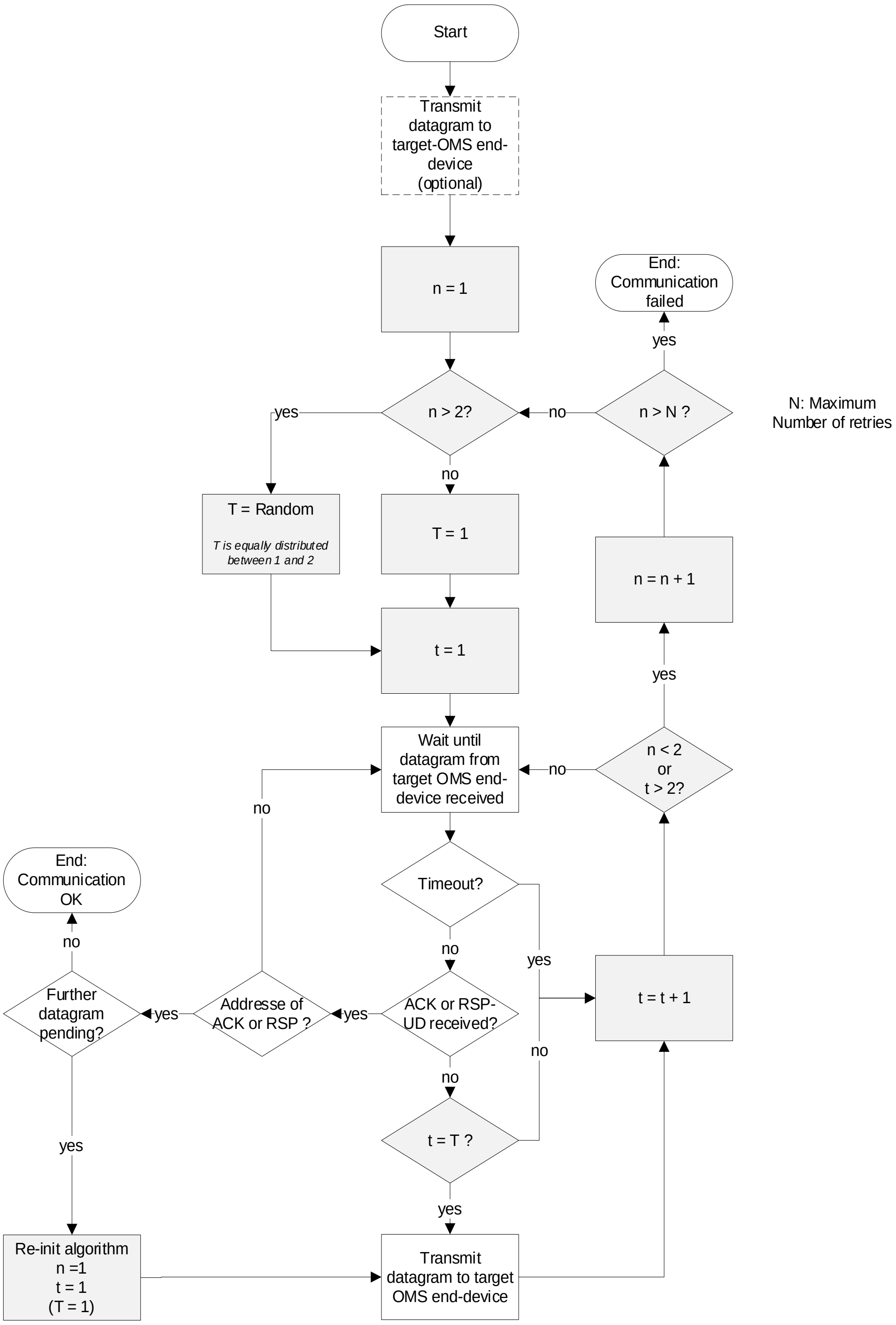


Figure I.1 - Collision avoiding algorithm

I.2 Explanation

Figure I.1 shows the procedure to transmit a message to a bidirectional OMS end-device including the retry-mechanism. The parameter N gives the maximum number of retries.

The retry-algorithm applies three variables:

n	Counts the number of tries to send the datagram
t	Counts the number of datagrams received during the actual try
T	Determines the datagram that will be followed by a transmission

In case of two unsuccessful tries resulting in n larger than 2, T is randomly chosen to 1 or 2 with a uniform distribution at the start of every (re-)try.

The basic idea is that within every try the interrogating device uses only one of two opportunities to transmit. This means that for both the first and second try the very first opportunity is used and for all following tries it would be either the first or the second one. The unused opportunity reduces the collision probability for competing devices and therefore contributes to a recovery of the overall-system.

A transmission to the addressed module is only performed under certain conditions. Of course, the general condition is the reception of a datagram from the target OMS end-device to meet the following listen-after-talk window. The algorithm evaluates furthermore, if the datagram is related to an already ongoing conversation, which is the case if the datagram is an acknowledgment or a response. In this case, it is further evaluated if this datagram is addressed to the interrogating device trying to send a transmission. If not, the device keeps on listening in order to leave this other conversation undisturbed. In case the ACK or RSP is dedicated to the device, the previous transmission is considered as successfully transmitted[7].

If the received datagram is neither part of another conversation nor the confirmation that a previous datagram was received, this would be an opportunity to send the datagram in case t equals T. Again, this latter additional condition resolves collision-scenarios with several devices transmitting simultaneously.

I.3 Example: Access of One Gateway without Collision

Assume a scenario with only one gateway addressing an OMS end-device with a sufficient radio propagation in-between. The algorithm is initialized with n = 1, t = 1 and T = 1. As a consequence, the very first received datagram from the target OMS end-device is followed by the gateway’s transmission. An ACK by the OMS end-device, which should be received in a collision-free environment, confirms the reception and results in the transmission of the next datagram by the gateway. Therefore, compared to a system without the retry-mechanism, the performance in terms of latency or throughput is not influenced in any way.

Figure I.2 shows this behaviour versus time together with the three variables of the algorithm.

[7] Based on the assumption, that the access-counter of the response can be used to match the answer of the interrogated module to the query.

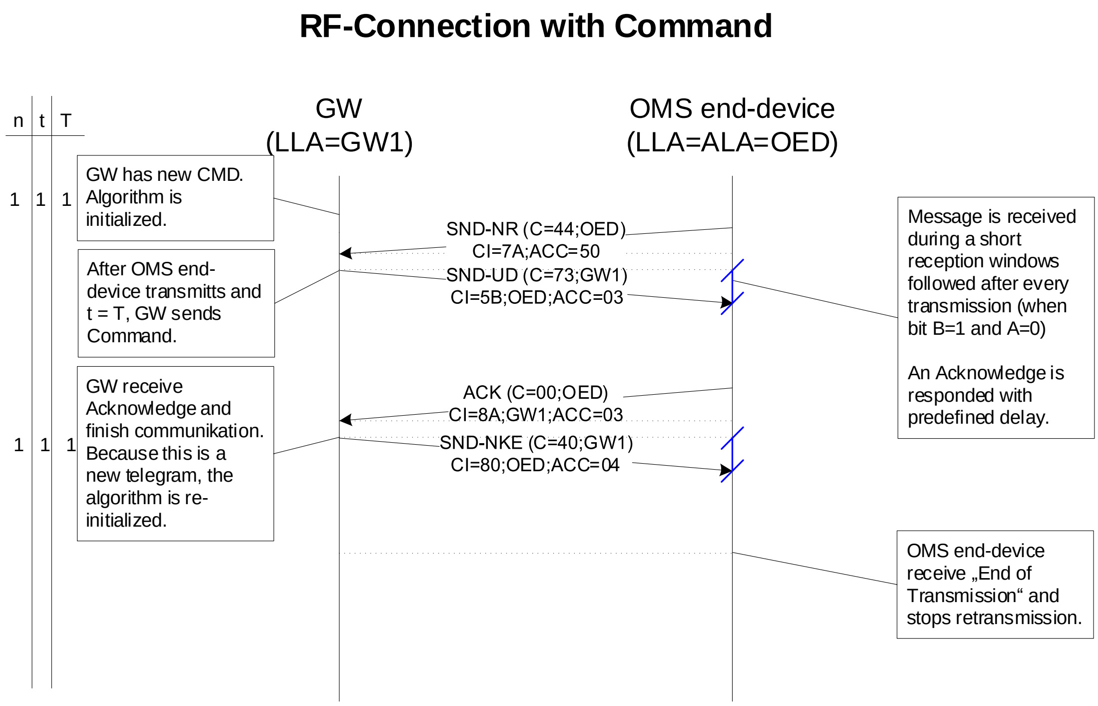


Figure I.2 – Timing diagram without collisions

I.4 Example: Access of Two Gateways with Collision

Assume a scenario with two gateways and an OMS end-device, again with sufficient and equal radio propagation between the gateways and the OMS end-device. Due to some reason, on both gateways a command appears to be sent to the OMS end-device. Note that it cannot be sent immediately in case the OMS end-device's receiver is not always on. Therefore, this scenario applies even in case of minutes between the appearances of the commands if the addressed OMS end-device has not transmitted since then, meaning that there was no opportunity to transmit the command.

Both gateways initialize the algorithm in the same way. In our assumption the received field strength of both gateways is equal at the OMS end-device and therefore the transmissions are jammed. Because the OMS end-device cannot receive any command in this case, there will not be an ACK by the module. Therefore, the number of received datagrams during this first try is increased to 2. This furthermore results in starting the next try by increasing n from 1 to 2. Also, for the second try, T is set to 1 (see Figure I.1) and therefore the very next opportunity is used, which again ends up in a collision. For the next try with n = 3, the random generator of every gateway determines T which now can be 1 or 2. Assuming a uniform distribution, there is a 50 % probability that two gateways choose different timeslots. This scenario is sketched in the following chart.

RF-Connection with Command

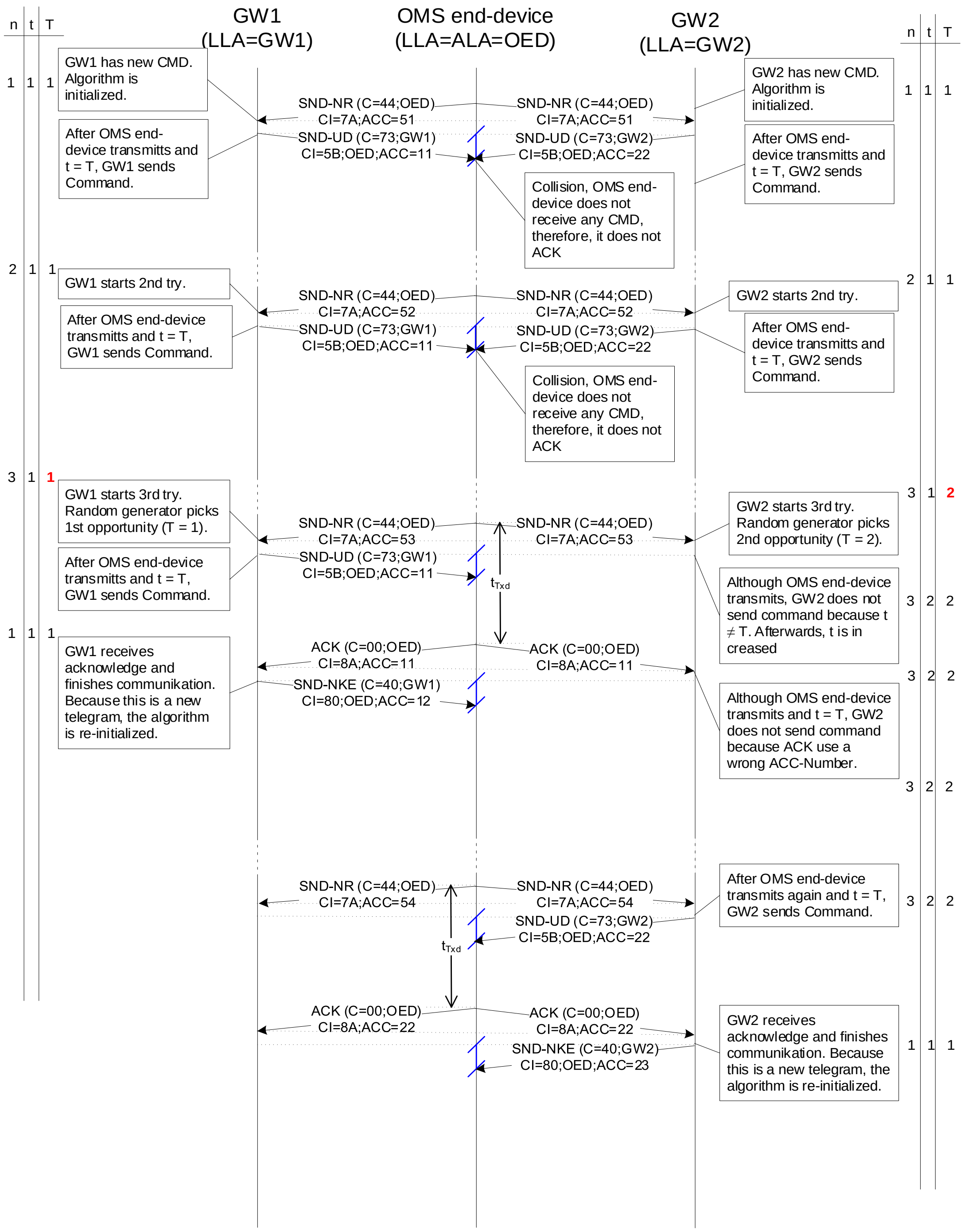


Figure I.3 – Timing diagram with collisions

After the collision of the gateways' first two transmissions, both start a 3rd try with GW1 choosing the 1st and GW2 the 2nd opportunity. As a result, GW1 transmits the command after the next received datagram, whereas GW2 waits for the next possibility. Because the following transmissions of the OMS end-device are dedicated to GW1, GW2 does not take these opportunities, although t is equivalent to T. Note that the received datagrams dedicated to another conversation do not result in incrementing t (see Figure I.1). After this conversation with GW1 is finished, GW2 takes the next datagram originating from the OMS end-device to transmit its pending datagram.

I.5 Collision Probabilities

If more than one interrogating device wants to send a command at the same time, this results always in a collision during the first two tries. If there are two devices, the probability to get a collision during the n^{th} try with n larger than 2 is $0,5^2 \times 2 = 0,5$.

$0,5^2$ is the probability that both devices choose the same opportunity and the multiplier 2 is reasoned by two possible opportunities. In general, the probability for collision is 1 in case of the first and second try and 0,5 for every other retries in case of two competing devices.

With the number of tries, the probability decreases that further tries are necessary. For example, the probability to have at least 3 tries is 1 and is the consequence of the 100 % collision probability for the 1st and 2nd try. The probability to have at least 4 tries is 1 × 1 × 0,5 and therefore the result of having a collision in the 1st, 2nd and 3rd try. In general, the probability to have the necessity for at least n tries is $1 \times 0,5^{n-2}$ (for n > 2).

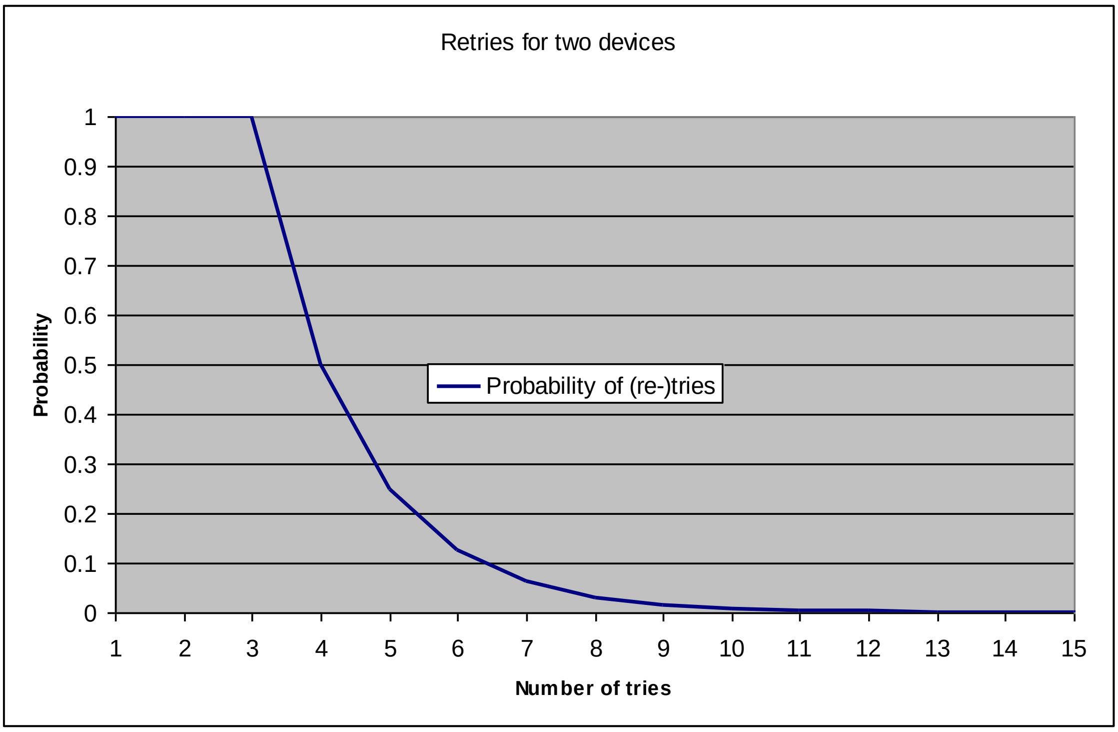
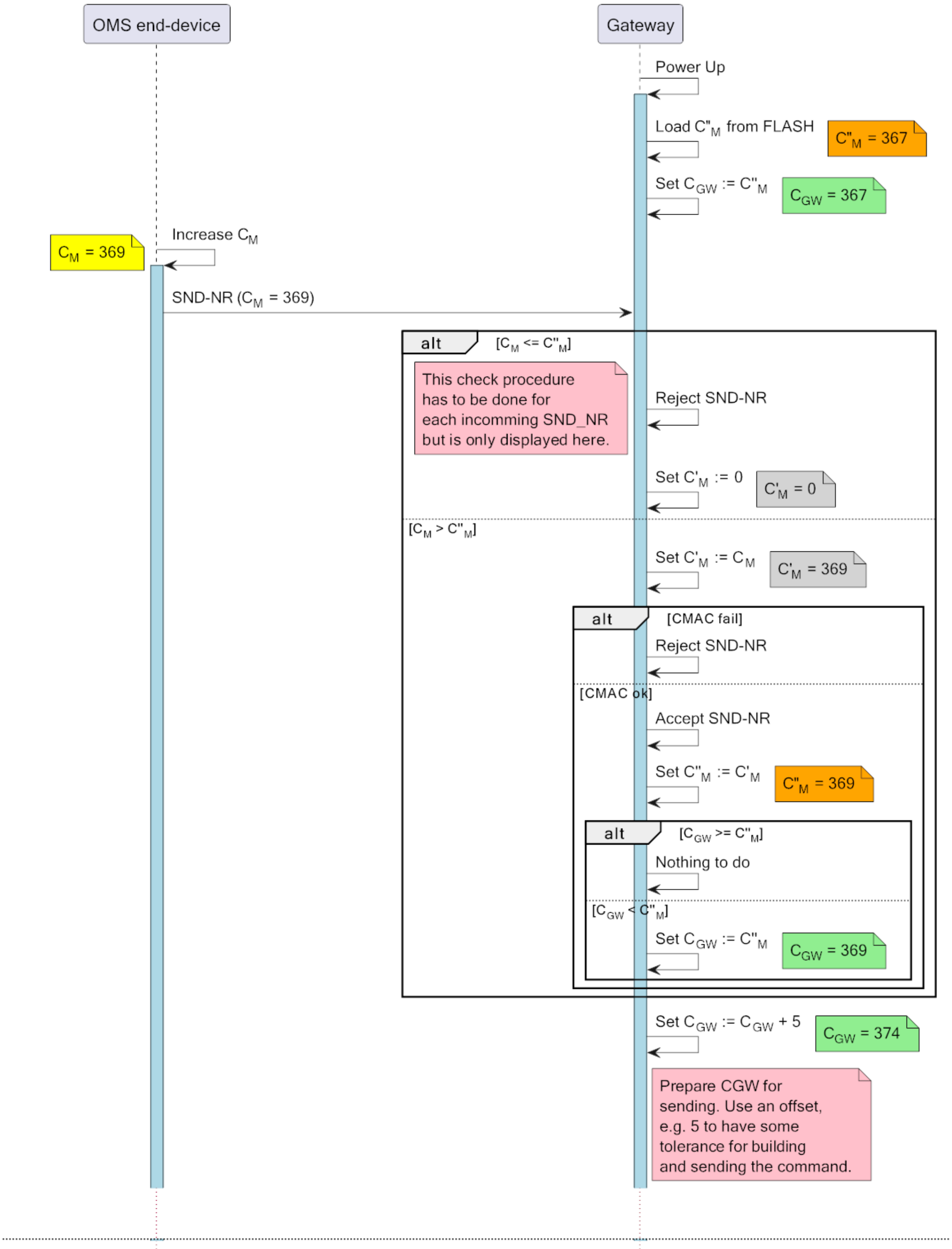
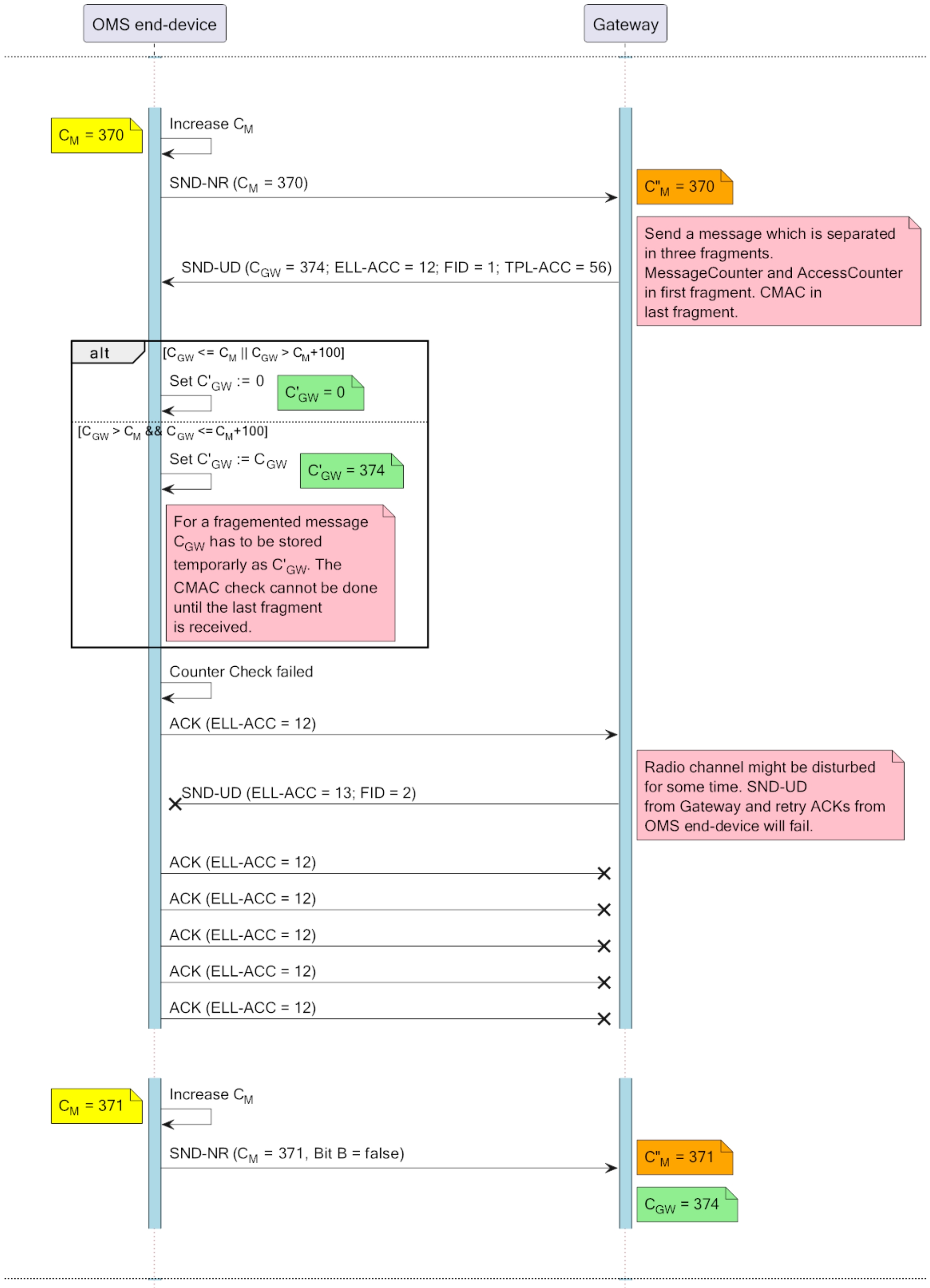


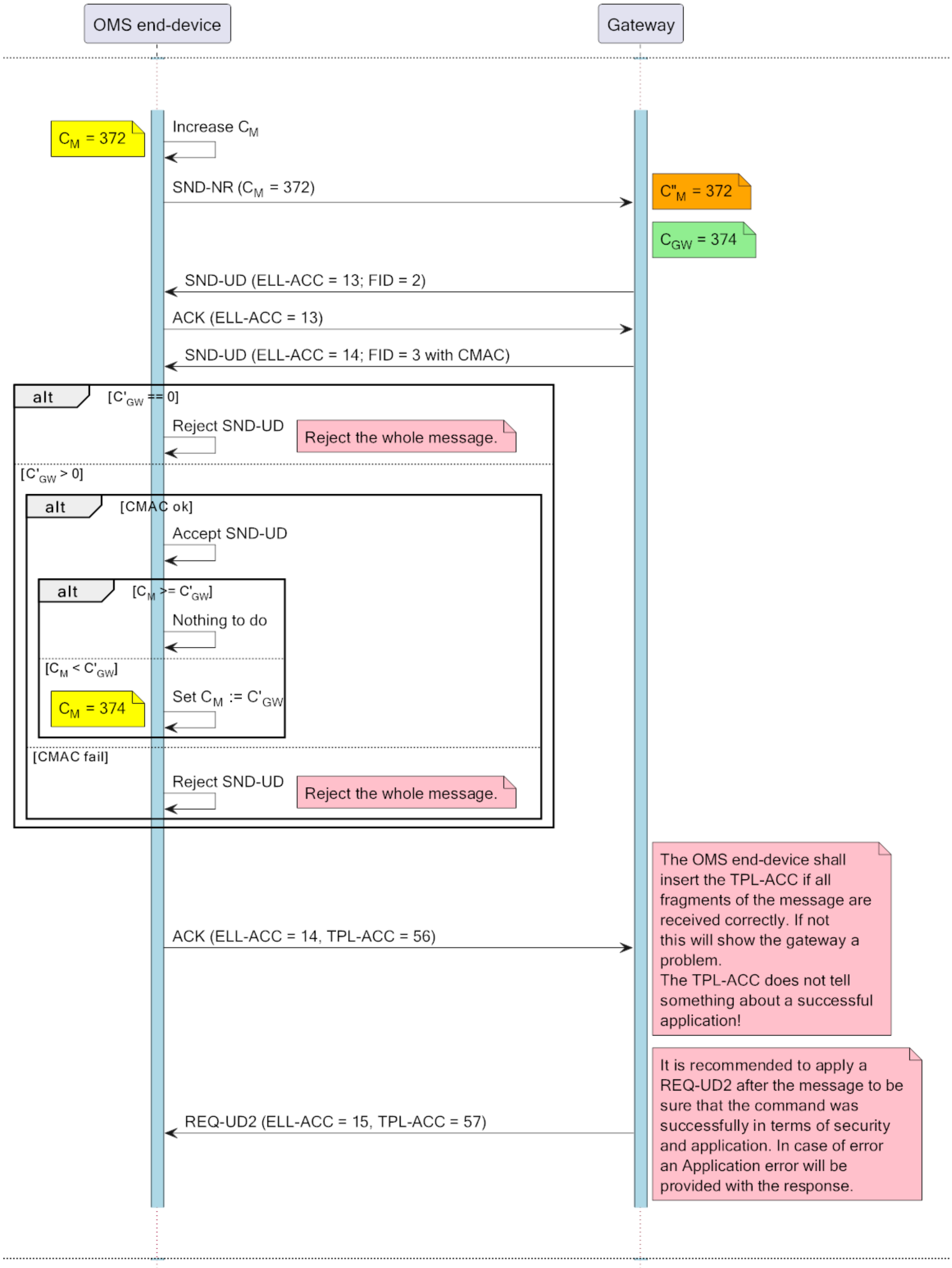
Figure I.4 – Collision probability

The probability for 12 tries or more is about 0,2 %, therefore a maximum number of N = 11 would be a suitable limit for the proposed algorithm. This limits the number of opportunities to a maximum of 1 + 1 + 9 × 2 = 20.

Annex J (Informative): Handling of Message Counter




OMS end-device
Gateway
C_M = 370
Increase C_M
SND-NR (C_M = 370)
C"_M = 370
Send a message which is separated in three fragments. MessageCounter and AccessCounter in first fragment. CMAC in last fragment.
SND-UD (C_GW = 374; ELL-ACC = 12; FID = 1; TPL-ACC = 56)
alt
[C_GW <= C_M || C_GW > C_M+100]
Set C'_GW := 0
C'_GW = 0
[C_GW > C_M && C_GW <= C_M+100]
Set C'_GW := C_GW
C'_GW = 374
For a fragemented message C_GW has to be stored temporarly as C'_GW. The CMAC check cannot be done until the last fragment is received.
Counter Check failed
ACK (ELL-ACC = 12)
SND-UD (ELL-ACC = 13; FID = 2)
Radio channel might be disturbed for some time. SND-UD from Gateway and retry ACKs from OMS end-device will fail.
ACK (ELL-ACC = 12)
ACK (ELL-ACC = 12)
ACK (ELL-ACC = 12)
ACK (ELL-ACC = 12)
ACK (ELL-ACC = 12)
C_M = 371
Increase C_M
SND-NR (C_M = 371, Bit B = false)
C"_M = 371
C_GW = 374


OMS end-device
Gateway
C_M = 372
Increase C_M
SND-NR (C_M = 372)
C"_M = 372
C_GW = 374
SND-UD (ELL-ACC = 13; FID = 2)
ACK (ELL-ACC = 13)
SND-UD (ELL-ACC = 14; FID = 3 with CMAC)
alt
[C'_GW == 0]
Reject SND-UD
Reject the whole message.
[C'_GW > 0]
alt
[CMAC ok]
Accept SND-UD
alt
[C_M >= C'_GW]
Nothing to do
[C_M < C'_GW]
C_M = 374
Set C_M := C'_GW
[CMAC fail]
Reject SND-UD
Reject the whole message.
The OMS end-device shall insert the TPL-ACC if all fragments of the message are received correctly. If not this will show the gateway a problem.
The TPL-ACC does not tell something about a successful application!
ACK (ELL-ACC = 14, TPL-ACC = 56)
It is recommended to apply a REQ-UD2 after the message to be sure that the command was successfully in terms of security and application. In case of error an Application error will be provided with the response.
REQ-UD2 (ELL-ACC = 15, TPL-ACC = 57)

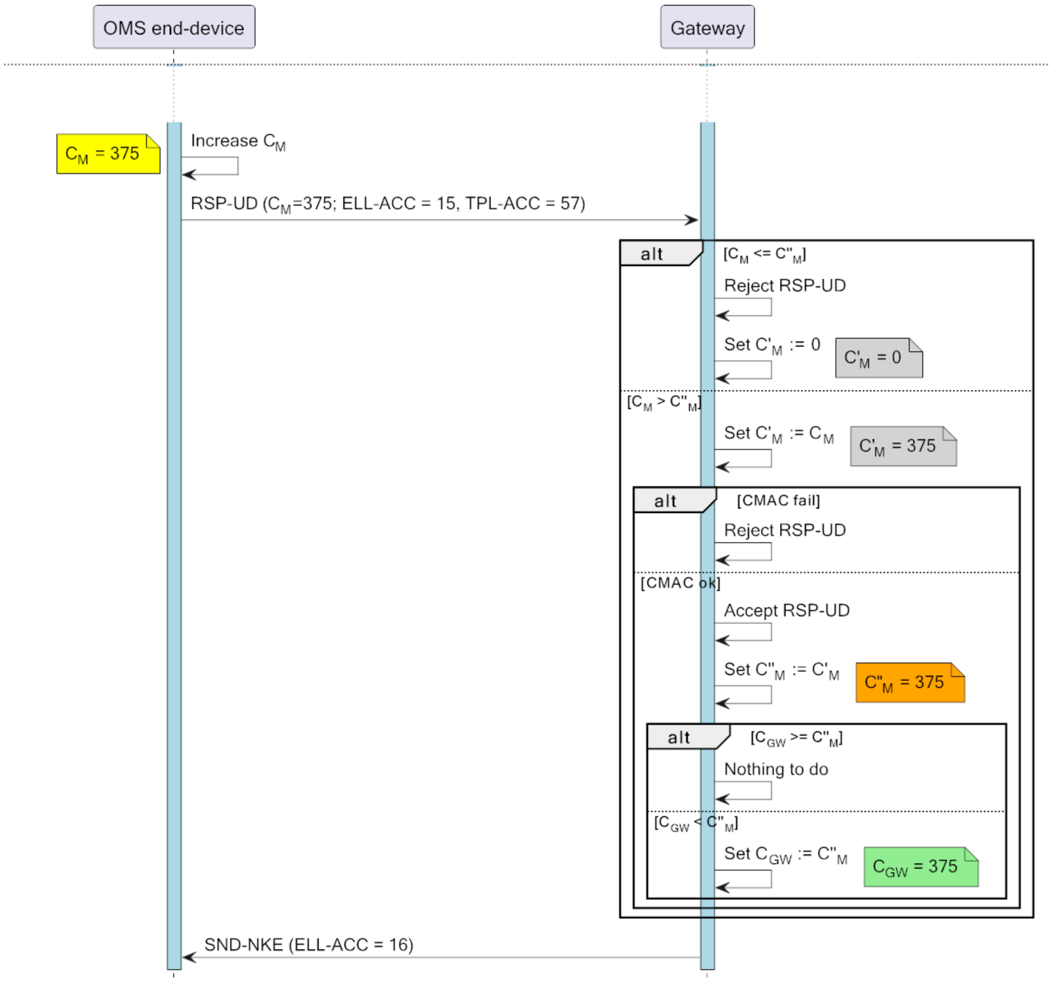


Figure J.1 – Example of message counter handling

Annex K (Normative): Descriptors

K.1 General

The purpose of a descriptor is the declaration of the meaning of DIB-elements in the individual device. Following DIB-elements of data points can be declared by descriptors.

Table K.1 – Overview of descriptors and related DIB-elements

DIB-element	Descriptor
Storage number	Storage interval descriptor
Tariff	Tariff descriptor
Subunit	Subunit descriptor

The link between the descriptor and the data point(s) is always the DIB-element. The DIB-element of a data point is identical to the DIB-element of the descriptor (see Table K.1). The values of the other DIB elements do not matter. For example, the subunit descriptor with a subunit of 1 is applicable for all data points with the same subunit regardless of its value of the DIB-elements storage number, tariff, or function.

A descriptor is valid for all DIB-elements in the device; e.g. the declaration of tariff number 1 shall be applied to all storage numbers and subunits.

A descriptor shall not change its definition over the lifetime of an OMS end-device. A new descriptor may be added for new data points during the lifetime of an OMS end-device. An existing descriptor may be deleted if the referenced data point is not used anymore.

K.2 Storage Descriptors

K.2.1 Storage Interval Descriptor

K.2.1.1 Usage

The storage interval descriptor declares the usage of a single storage number or a range of storage numbers for historical values. Historical values are one or several measurement values that have been generated in the past. Typically, historical values are generated periodically at a pre-set date and time like each full hour or at the end of a month. The OMS end-device may transmit either a single historical value (e.g. the value at the end of last month) or a set of historical values (e.g. the last 24-hourly values).

A single historical value is mostly transmitted together with a time stamp, which is linked with the historical value by the same storage number.

A set of historical data is transmitted either with a time stamp for each historical value or as a pure set of historical values with only a start date/time and an interval (refer to standard profile in [EN 13757-3:2018], Annex F.1).

The storage interval descriptor is used to declare the temporal relation between the values. In a set of historical values, it describes the applied interval between the values (e.g. one hour). In a single data point it declares the time when the next single historical value is expected (e.g. next new value of this storage number will be generated during a month).

K.2.1.2 Coding

The temporal relation shall be declared according to Table K.2.

Table K.2 – Declaration of Storage interval descriptors

M-Bus data point	VIB	Description
Storage interval year(s)	FDh 29h	Year
Storage interval month(s)	FDh 28h	Month
Storage interval [sec(s) … day(s)]	FDh 27h	Day
Storage interval [sec(s) … day(s)]	FDh 26h	Hour
Storage interval [sec(s) … day(s)]	FDh 25h	Minute
Storage interval [sec(s) … day(s)]	FDh 24h	Second

The value of the data point storage interval descriptor is coded as type B (according to [EN 13757-3:2018], Annex A). The value equals the used storage interval and is frequently 1. A storage interval of 0 describes that all values refers to the same point in time or that these values have no temporal relation.

In case of a single historical value, the storage interval descriptor uses the storage number of the data point.

In case of a standard profile, the storage interval descriptor uses the storage number of the oldest measurement value in the set of historical values.

In case of a compact profile, the storage interval descriptor uses the storage number of base time respectively base value.

The other DIB-elements tariff, function and subunit in the data point storage interval descriptor shall always be set to 0.

K.2.1.3 Scope of Application

The storage interval descriptor is mandatory for all historical values, except for

- All MB-Tags listed in Annex A,
- Historical values providing a time stamp for each used storage number,
- Storage numbers using a final DIFE (assignment is done by register-ID),
- Transmissions with compact profile according to Annex G (Note that any compact profile can be converted to a set of historical values with timestamps).

Storage number 0 (without final DIFE) is exclusively being used for current values and values without a temporal relation, e.g. the fabrication number. It is not permitted to use the storage interval descriptor for storage number 0.

Storage number 1 (without final DIFE) is being used for due date values. As long as the due date is provided no storage interval descriptor is required.

K.2.2 Storage Range Descriptor

Table K.3 – Declaration of Storage range descriptors

M-Bus data point	VIB	Description
First storage number for cyclic storage	FDh 20h	Time point for start of range (oldest value)
Last storage number for cyclic storage	FDh 21h	Time point for end of range (newest value)
Size of storage block	FDh 22h	Number of applied storage numbers

The storage range descriptor FDh 21h uses the storage number of the newest value in the load profile. The storage range descriptors FDh 20h and FDh 22h use the storage number of the oldest value in the load profile. The data point sub fields for tariff, function, and subunit in the data point storage range descriptor shall be set to 0. The storage range descriptors FDh 20h and FDh 21h do not transmit values.

The transmission of a storage range descriptors is generally optional, with a few exceptions.

Under the following conditions the use of the storage range descriptor is mandatory:

1. If several sets of historical values with more than one pair of values are transmitted, a storage range descriptor according to Table K.3 shall be included in the message. All sets in this message shall use the same type of storage range descriptor.
2. If the storage number of the oldest value in a set of historical values is not the smallest storage number in this set, then this storage number shall be declared with the storage range descriptor FDh 20h.

K.3 Subunit Descriptor

The subunit descriptor declares the usage of the subunit number.

The subunit descriptor is coded with 01h FDh 23h xx. The values for xx are listed in Table K.4.

NOTE: The VIB of the subunit descriptor is the same as for the tariff descriptor.

Table K.4 – Subunit index values for the subunit descriptor

Index value	Description	Media type	Comment
0	Main register, legacy	all	
1	OBIS value group B = 1	electricity meter	
2	OBIS value group B = 2	electricity meter	
3	OBIS value group B = 3	electricity meter	
4	OBIS value group B = 4	electricity meter	
5	Tariff subunit	all	
6	Minimum subunit	all	
7	Maximum subunit	all	
8	Data logger	all	
9	Event logger	all	e.g. error logging
10	Test subunit/test mode	all	Test results
11	Calibration subunit	all	Calibration results
12	Adjustment subunit	all	Adjustment values
13..20	Pulse collector 1…8	all	
21…29	Configuration subunit/configuration mode	all	
30…99	Reserved		
100…127	Manufacturer specific	all	
128…255	Reserved for other descriptors		

It is not permitted to use the subunit descriptor for the subunit value 0. The transmission of the subunit descriptors is mandatory for all subunit values greater than 0. For the case of a Subunit index value of 0 the transmission of the subunit descriptors may be omitted.

The subunit descriptor shall use the subunit number of the declared subunit. The DIB-elements storage number, function and tariff in the data point 'subunit descriptor' shall be set to 0.

K.4 Tariff Descriptor

The tariff descriptor declares the usage of the tariff register number.

The tariff descriptor is coded with 01h FDh 23h xx. The values for xx are listed in Table K.5.

NOTE: The VIB of the tariff descriptor is the same as for the subunit descriptor.

Table K.5 – Tariff index values for the tariff descriptor

Index value	Description	Device type	Comment
0…127	Reserved for other descriptors		
	General tariffs		
128…139	Manufacturer specific		
140…149	Reserved		
	Time based tariffs		
150	Absolute time of day	All	e.g. 8:00 to 11:00 each day
151	Weekdays	All	e.g. each Saturday and Sunday
152	Days in Month	All	e.g. each 15th.
153…159	Reserved		
	Threshold based tariffs		
160	Difference temperature	Heat, Cold	
161	Forward temperature	Heat, Cold,	
162	Return temperature	Heat, Cold	
163	Return temperature threshold for calculation of theoretical energy	Heat, Cold	[a]
164	Volume Flow	Water, Heat, Cold, Gas	
165	Power	Electricity, Heat, Cold	
166…189	Reserved		
	Consumption based tariffs		
190	Energy consumption	Electricity, Heat, Cold	e.g. after consumption of 100 kWh
191	Volume consumption	Water, Heat, Cold, Gas	
192	Financial consumption	All	e.g. prepaid tariffs
193…209	Reserved		
	Combined tariffs		
210	Time and threshold based		
211	Time and consumption based		
212	Threshold and consumption based		
213…229	Reserved		

Table K.5 (continued)

Index value	Description	Device type	Comment
	Other tariffs		
230	Energy positive	Electricity, Heat, Cold	
231	Energy negative	Electricity, Heat, Cold	
232	Energy heating	Heat, Cold,	
233	Energy cooling	Heat, Cold,	
234	External input 1	All	Controlled by user from outside
235	External input 2	All	
	Reserved		
236…249	Reserved		
250…255	Reserved for table extension		

[a] The energy is accumulated in tariff registers depending on the return (outlet) temperature. The quantity of this energy results from a mathematical calculation is based on the difference of return (outlet) temperature and a pre-defined return temperature threshold. It can be distinguished between accumulated energy in case the return temperature is lower or higher than the return threshold value. This can be signaled with the orthogonal VIFE 40h or 48h.

It is not permitted to use the tariff descriptor for the tariff value 0. The transmission of tariff descriptors is mandatory for all tariff values greater than 0, except for the following conditions:

- A combined heat/cooling meter uses the tariff register 1 for the cooling energy.
- All MB-Tags listed in Annex A

The tariff descriptor shall use the tariff register number of the declared tariff. The DIB-elements storage number, function and subunit in the data point 'tariff descriptor' shall be set to 0.

K.5 Examples

K.5.1 Example: Storage Descriptor

Table K.6 – Example load profile for storage descriptor

1st value at the end of the month	2008-01-31	65 litres (10^{-3} m³)
2nd value at the end of the month	2008-02-29	209 litres
3rd value at the end of the month	2008-03-31	423 litres
4th value at the end of the month	2008-04-30	755 litres
Last value at the end of the month	2008-05-31	1013 litres

Table K.7 – Example for coding of the storage descriptor

DIB		**VIB**	**Data**	**Hex coded (LSByte first)**
Data field	**Storage number**			
2 digit BCD	8	Size of storage block	5	`89 04 FD 22 05`
2 digit BCD	8	Storage Interval Descriptor months	1	`89 04 FD 28 01`
16 bit binary	12	Date (Type G)	2008-05-31	`82 06 6C 1F 15`
8 digit BCD	8	Volume (litres)	65	`8C 04 13 65 00 00 00`
8 digit BCD	9	Volume (litres)	209	`CC 04 13 09 02 00 00`
8 digit BCD	10	Volume (litres)	423	`8C 05 13 23 04 00 00`
8 digit BCD	11	Volume (litres)	755	`CC 05 13 55 07 00 00`
8 digit BCD	12	Volume (litres)	1013	`8C 06 13 13 10 00 00`
0 bit	12	Storage Range Descriptor “End”	-	`80 06 FD 21`

K.5.2 Example: Subunit Descriptor

The following definition links subunit 2 to a data logger: 81h 80h 40h FDh 23h 08h

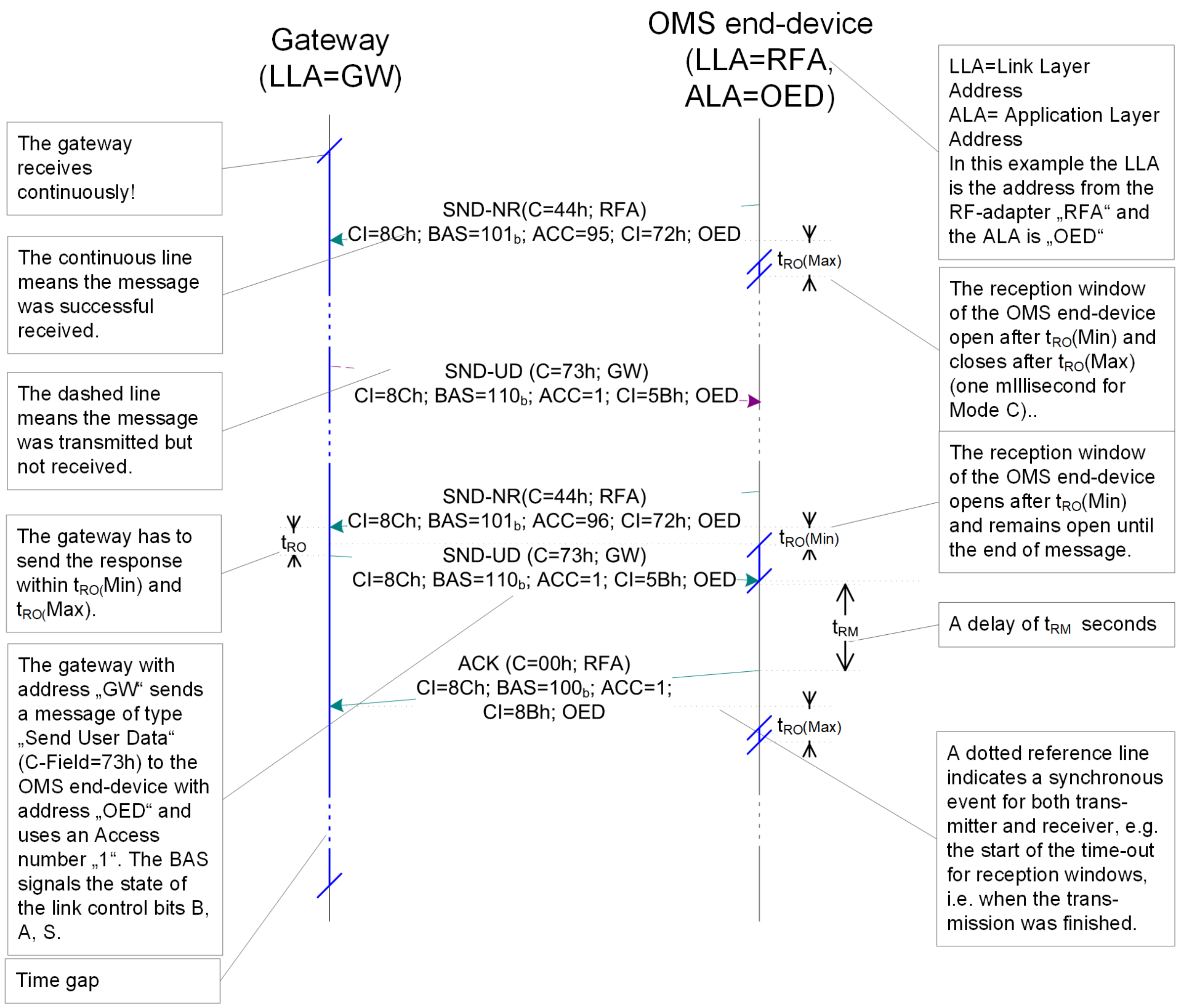
K.5.3 Example: Tariff Descriptor

The following definition links tariff 3 to the threshold based tariff “Difference Temperature”: 81h 30h FDh 23h A0h

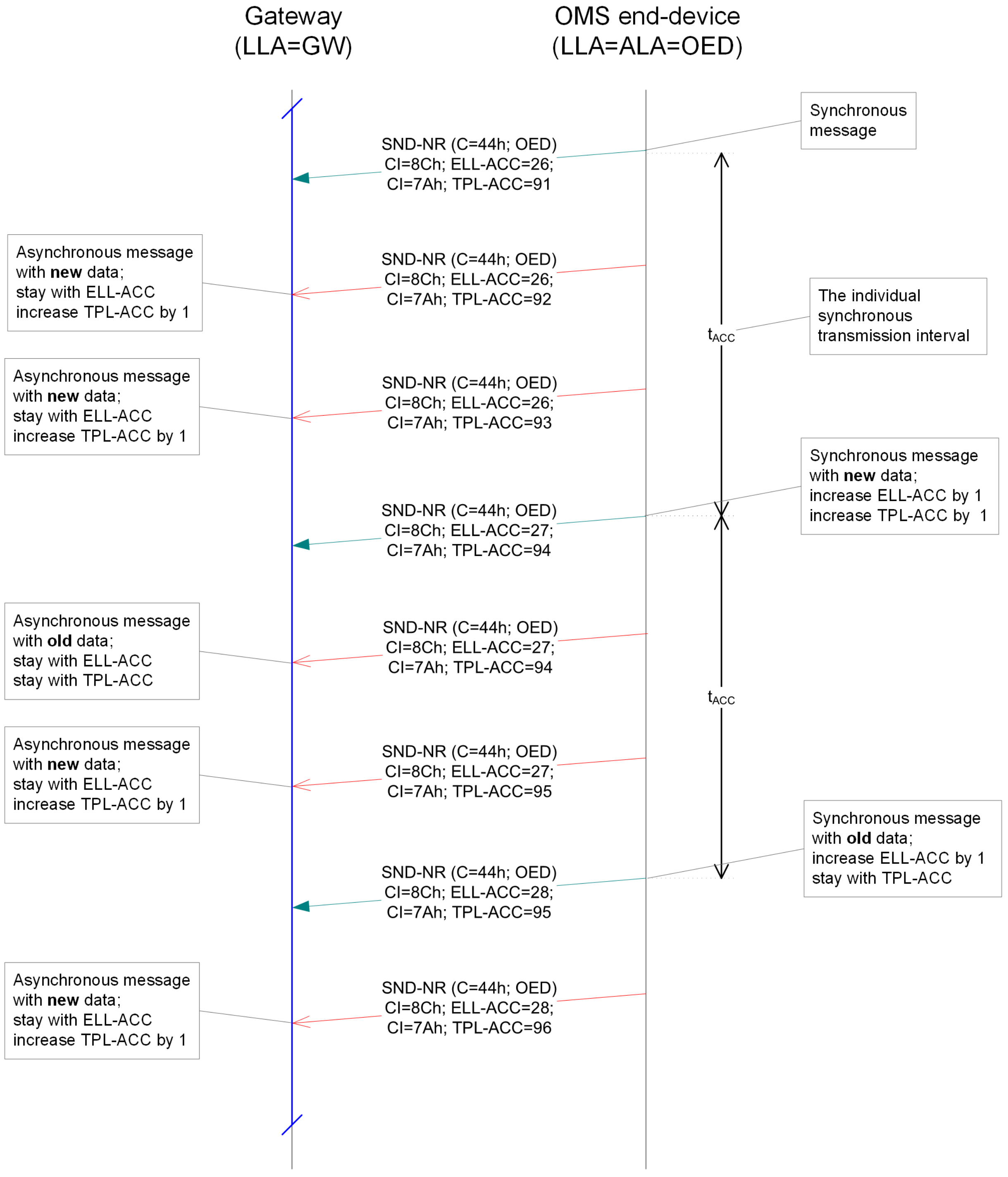
Annex L (Informative): Timing Diagram

The next pages show examples of Timing diagrams for Mode C. If the Access Number is not explicitly declared, then the shown Access number is the Access Number of the ELL or of the TPL (if the ELL does not exist).

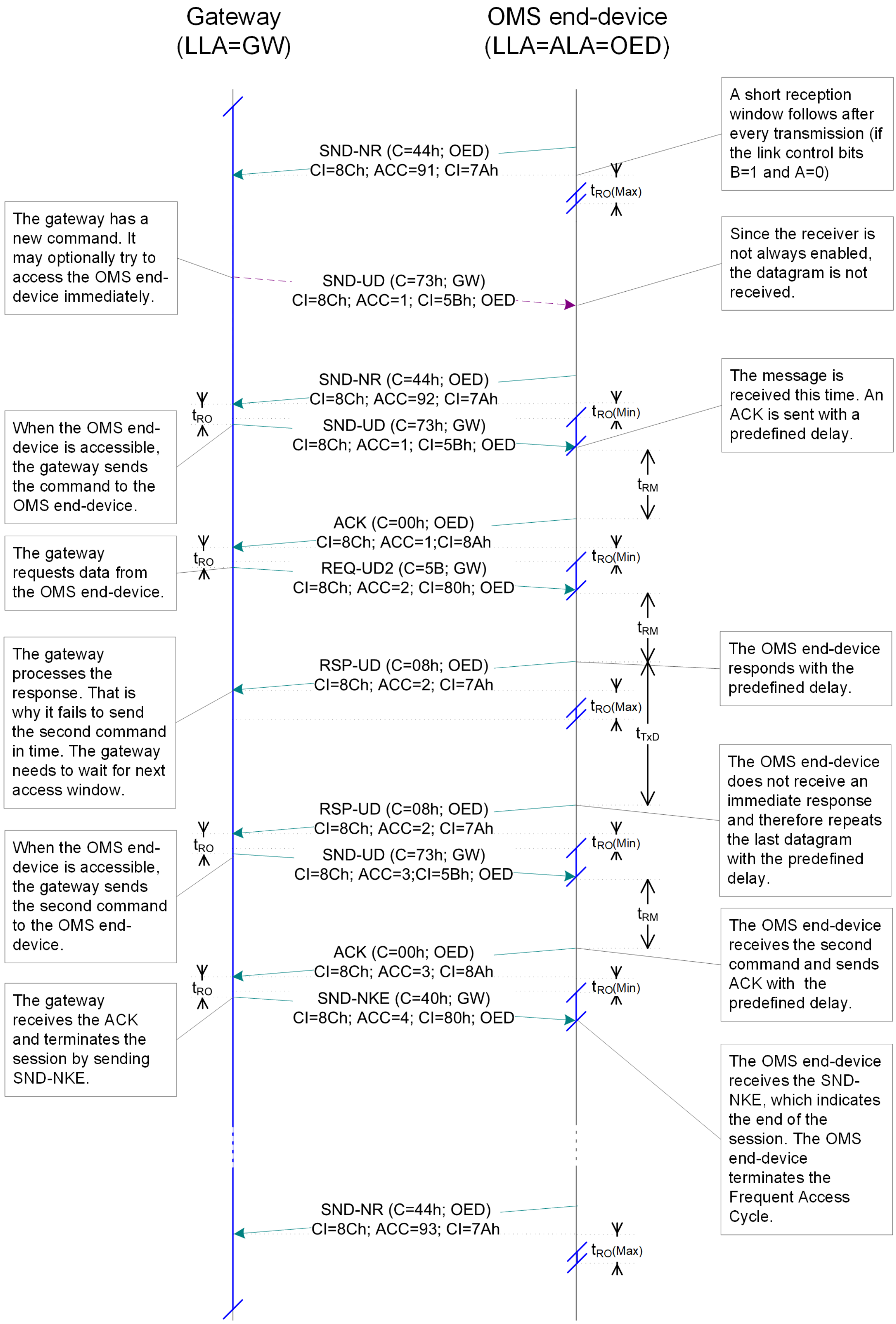
5 ## L.1 Legend



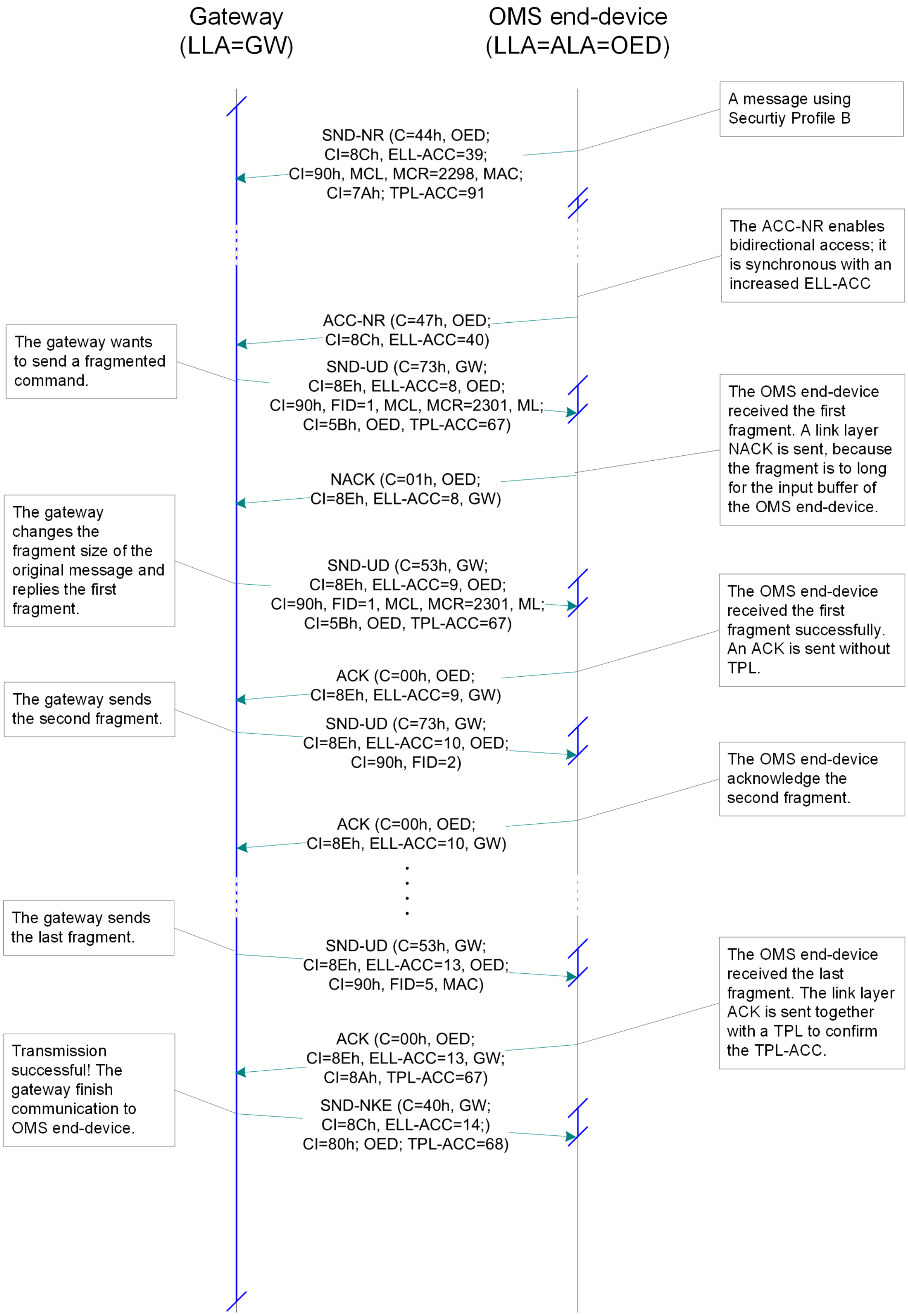
L.2 Unidirectional OMS end-device with Synchronous and Asynchronous Transmission



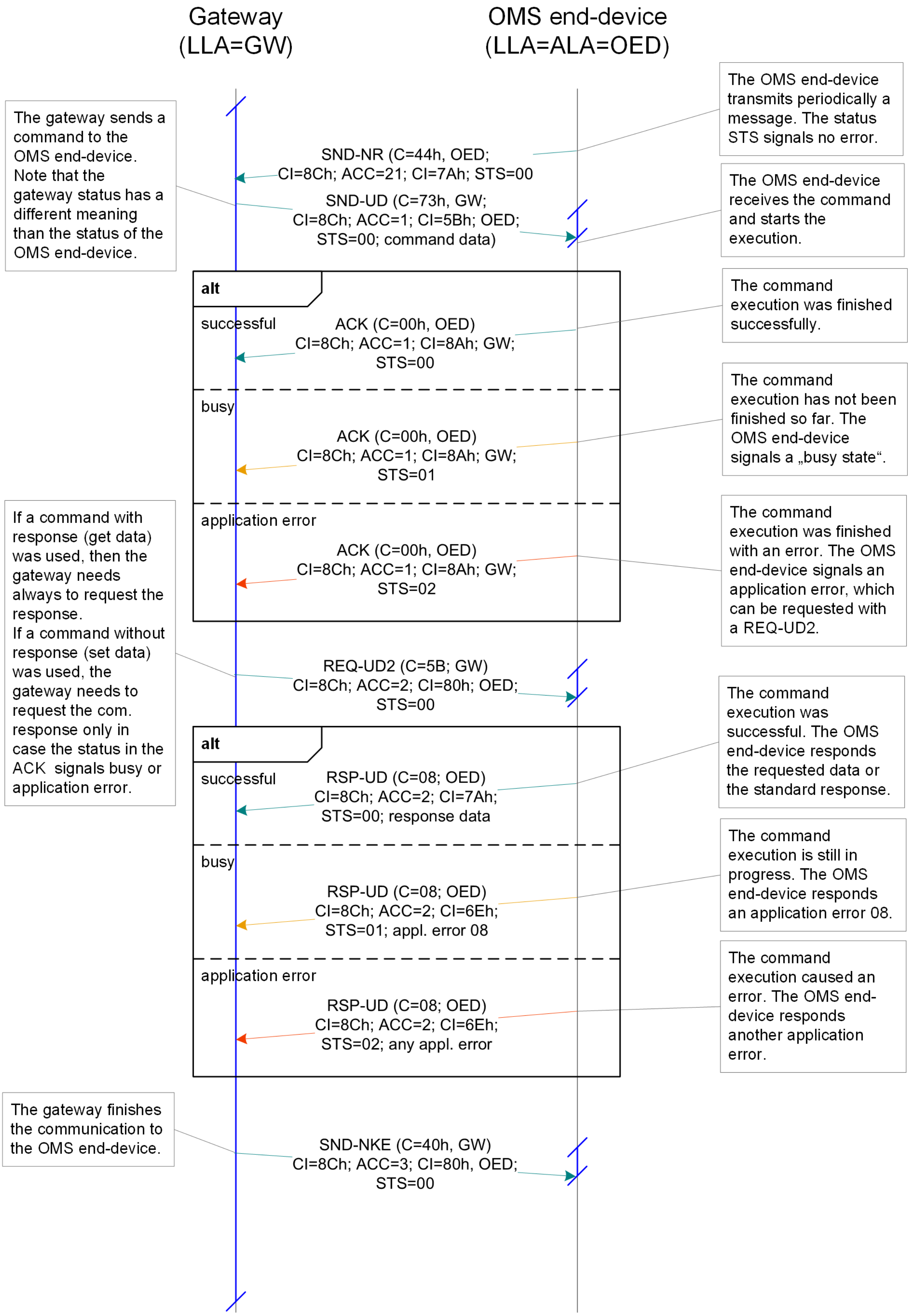
L.3 RF-Connection with SND-UD and Short TPL



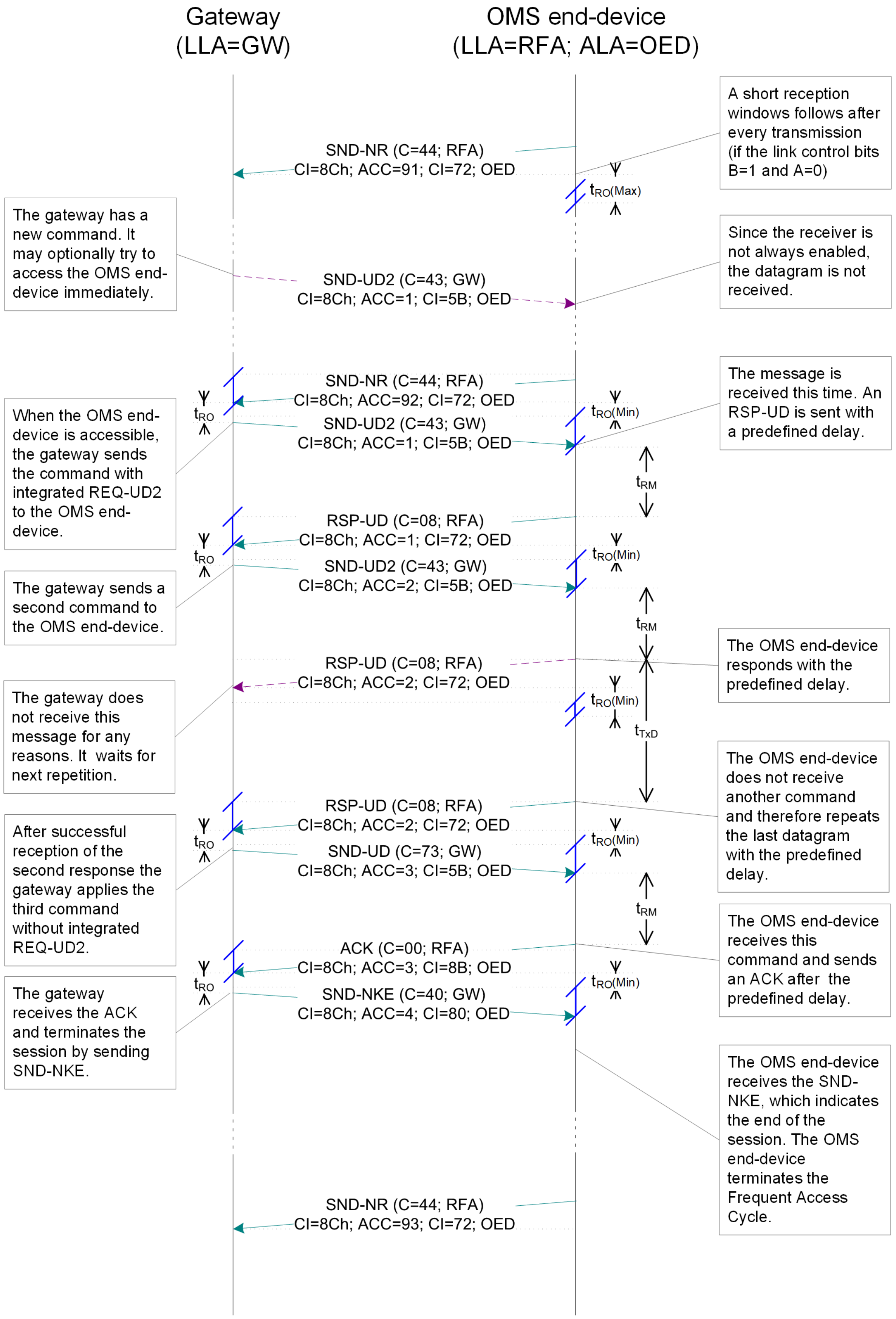
L.4 Transmission of Fragmented Message with SND-UD



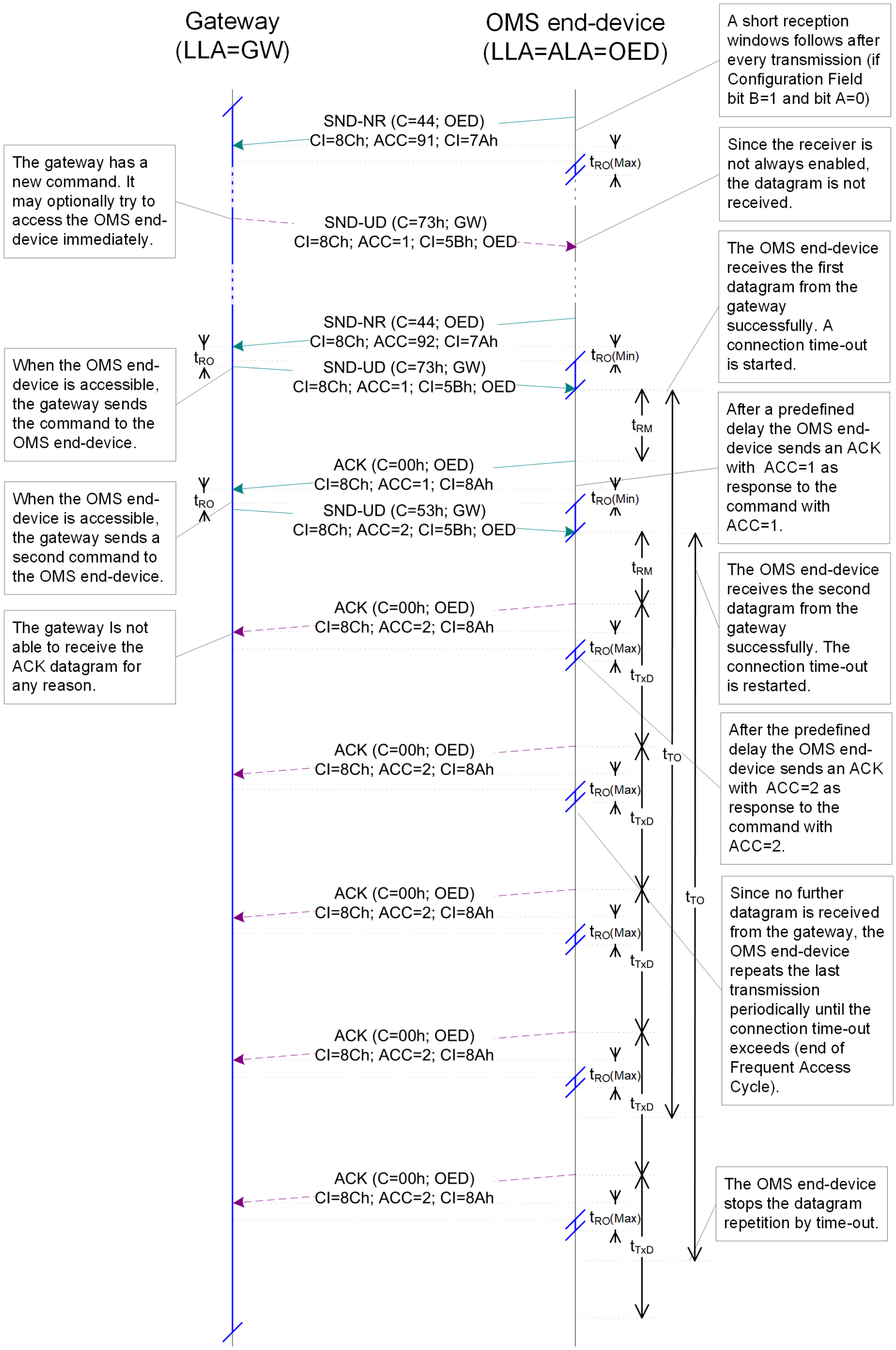
L.5 Transmission of ACK + RSP-UD with Different Command States



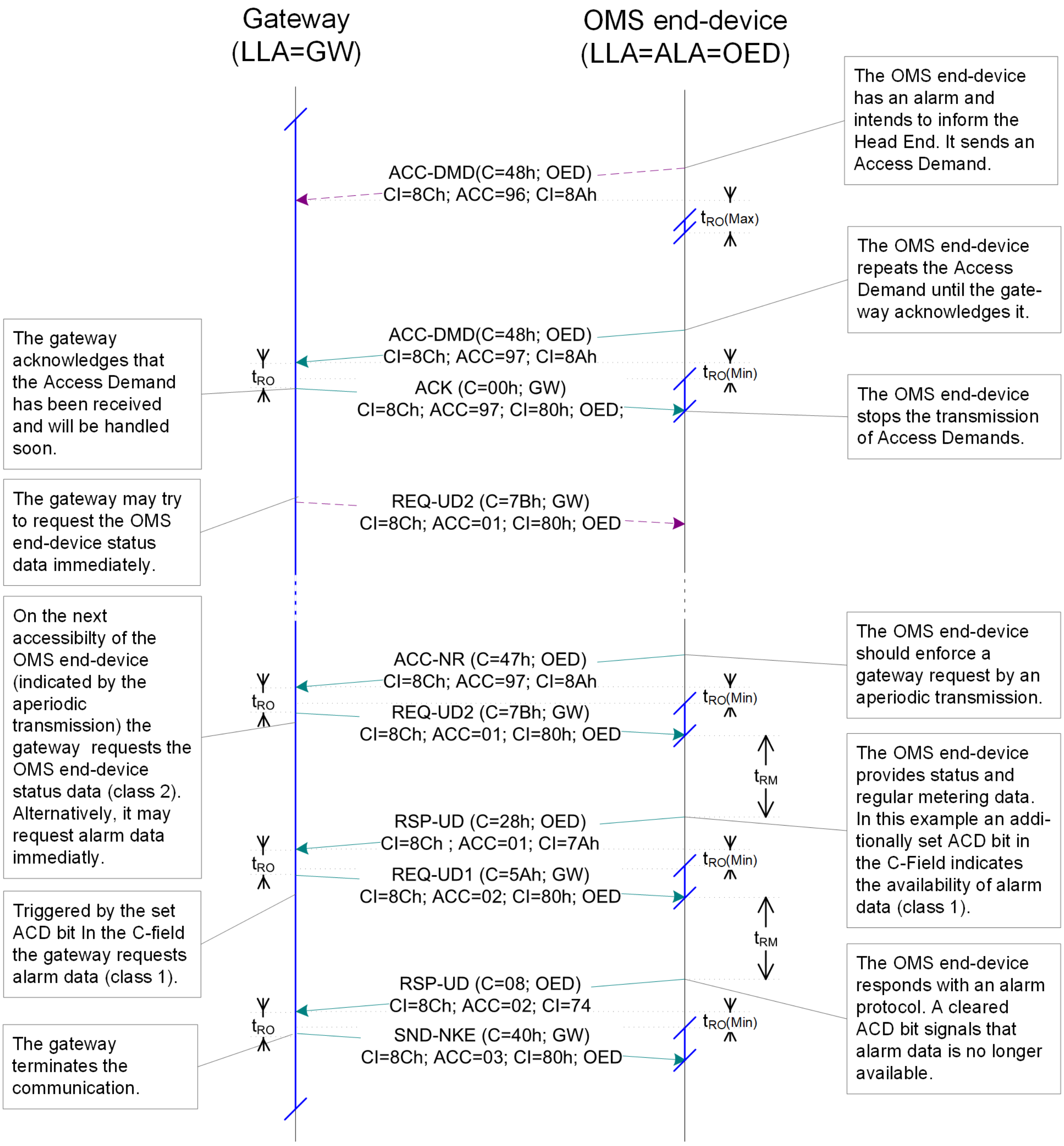
L.6 RF-Connection with SND-UD2 and Long TPL



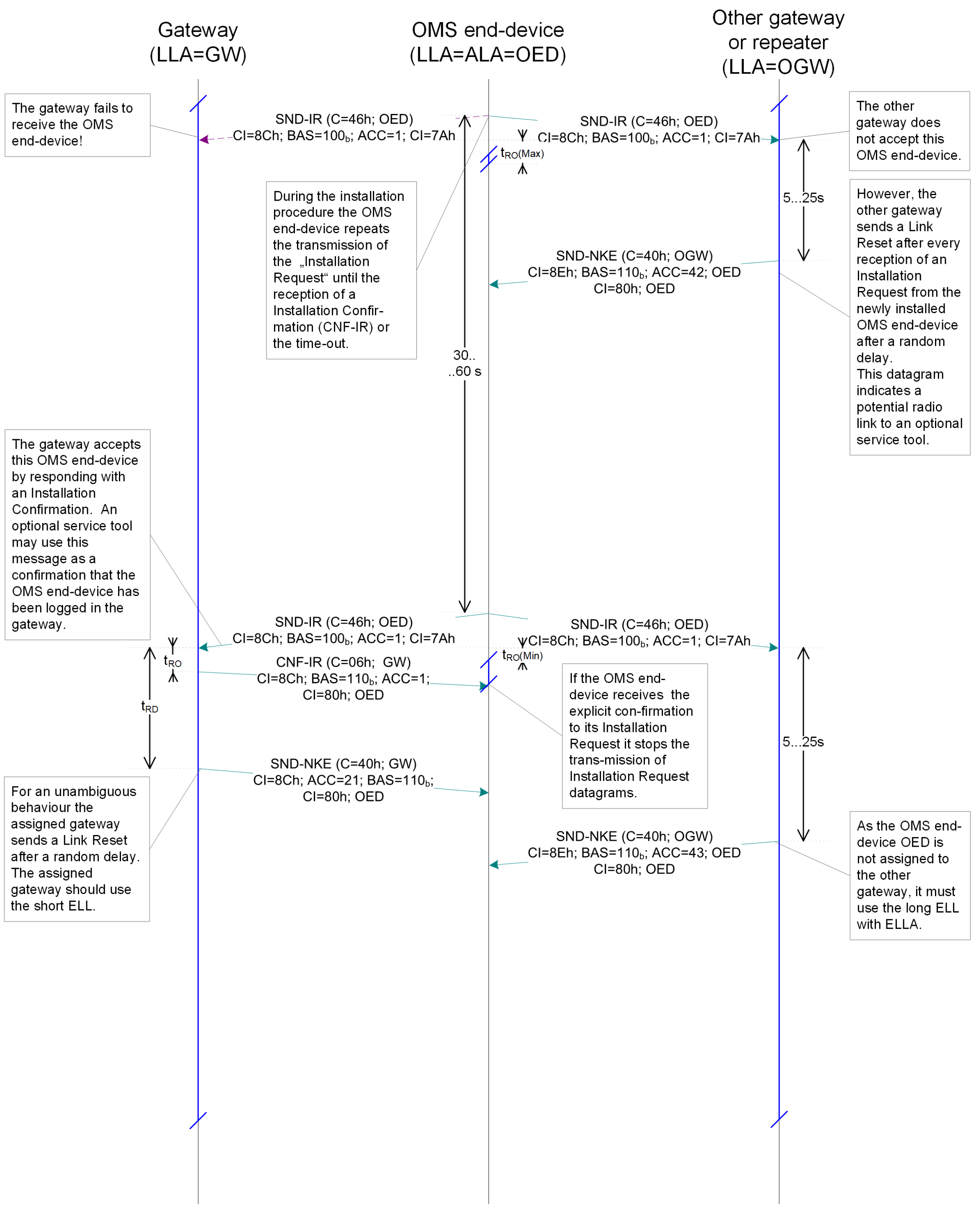
L.7 Connection Timeout of the Frequent Access Cycle



L.8 Access Demand from OMS end-device



L.9 Installation Procedure



Annex M (Normative): Requirements for OMS Use Case Support

This annex contains specifications of interoperable OMS use cases of OMS end-devices. The set of optional use cases support for example clock management, disconnect/reconnect, key management, firmware update etc.

The annex in addition contains general introduction to basic communication sequences for both wired and wireless M-Bus to support these use cases.

The OMS end-device support for specific use cases is declared by the manufacturer in the [ManDec].

This annex may be subject to a more frequent update than this main document. Therefore, the annex is not included. The current version (Release C or later) can be downloaded from the OMS website (www.oms-group.org).

Annex N (Informative): Datagram Examples for Wired M-Bus and Wireless M-Bus

This annex lists several message examples for wired and wireless M-Bus. Be aware that this is an informative annex. In case of deviation between this annex and the normative specification, the content of specification has to be applied.

For the sake of better readability this annex is not included.

The current version (Release E or later) can be downloaded from the OMS website (www.oms-group.org).

Annex O (Informative): Alternative Physical Layers for OMS

Countries outside the CEPT may have defined other frequencies than those covered in the OMS-PC. OMS gives a recommendation on the usage of alternative Physical Layers and the country specific parameters.

Annex O may be subject to a more frequent change than this main document. Therefore, the annex is not included. The current version (Release B or later) can be downloaded from the OMS website (www.oms-group.org).

Annex P (Normative and Informative): Requirements for Wired M-Bus

Annex P describes the Open Metering System requirements for the wired M-Bus. The wired M-Bus is normatively represented in the [EN 13757-2], [EN 13757-3] and [EN 13757-7] standard. During application of the EN 13757 standard, a certain amount of scope for interpretation or design freedom is offered. Among other things, this factor applies to the coding of the data within the application layer.

This annex may be subject to a more frequent update than this main document. Therefore, the annex is not included. The current version (Release C or later) can be downloaded from the OMS website (www.oms-group.org).

Annex Q (Normative): OMS LPWAN

This annex provides all definitions for the wireless M-Bus mode OMS LPWAN.

This annex may be subject to a more frequent update than this main document. Therefore, the annex is not included. The current version (Release A or later) can be downloaded from the OMS website (www.oms-group.org).

Annex R (Normative): Meter Reading Transmission via M-Bus Compact Profile; to meet BSI TR-03109-1 TAF7

This annex provides the definitions for the OMS specific meter reading transmission for BSI TAF7. This implementation is in line with [BSI TR-03109-1] version 1.1.

This annex may be subject to a more frequent update than this main document. Therefore, the annex is not included. The current version (Release A or later) can be downloaded from the OMS website (www.oms-group.org).