



BSI Standards Publication

Communication systems for meters

Part 7: Transport and security services

National foreword

This British Standard is the UK implementation of EN 13757-7:2018. Together with PD CEN/TR 17167:2018 and BS EN 13757-3:2018, it supersedes BS EN 13757-3:2013, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee PEL/894, Remote Meter Reading.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 93564 0

ICS 33.200; 35.100.10; 35.100.20

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 May 2018.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

English Version

Communication systems for meters - Part 7: Transport and security services

Systèmes de communication pour compteurs - Partie 7
: Services de transport et de sécurité

Kommunikationssysteme für Zähler - Teil 7:
Transport- und Sicherheitsdienste

This European Standard was approved by CEN on 8 February 2018.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Contents

Page

European foreword.....	5
Introduction	7
1 Scope	9
2 Normative references	9
3 Terms and definitions	10
4 Abbreviations and symbols	12
4.1 Abbreviations	12
4.2 Symbols.....	14
5 Layer model.....	14
5.1 M-Bus Layers.....	14
5.2 The CI-field principle	15
6 Authentication and Fragmentation Sublayer (AFL)	19
6.1 Introduction	19
6.2 Overview of the AFL-Structure	20
6.3 Components of the AFL.....	21
6.3.1 AFL Length Field (AFL.AFLL)	21
6.3.2 AFL Fragmentation Control Field (AFL.FCL).....	21
6.3.3 AFL Message Control Field (AFL.MCL)	22
6.3.4 AFL Key Information-Field (AFL.KI)	23
6.3.5 AFL Message counter field (AFL.MCR)	23
6.3.6 AFL MAC-field (AFL.MAC)	24
6.3.7 AFL Message Length Field (AFL.ML)	24
7 Transport Layer (TPL)	24
7.1 Introduction	24
7.2 Structure of none TPL header.....	25
7.3 Structure of short TPL header	25
7.4 Structure of long TPL header	25
7.5 CI-field dependent elements	25
7.5.1 Identification number	25
7.5.2 Manufacturer identification.....	26
7.5.3 Version identification.....	26
7.5.4 Device type identification	26
7.5.5 Access number	28
7.5.6 Status byte in meter messages	30
7.5.7 Status byte in partner messages.....	31
7.5.8 Configuration field.....	32
7.6 Configuration field dependent structure.....	33
7.6.1 General.....	33
7.6.2 Configuration field extension	34
7.6.3 Optional TPL-header fields.....	34
7.6.4 Optional TPL Trailer fields	34
7.6.5 Partial encryption	34

7.7	Security mode specific TPL-fields.....	34
7.7.1	Shared subfields of configuration field and configuration field extension	34
7.7.2	Configuration field of Security mode 0	37
7.7.3	Configuration field of Security modes 2 and 3	38
7.7.4	Configuration field of Security mode 5	39
7.7.5	Configuration field of Security mode 7	40
7.7.6	Configuration field of Security mode 8	41
7.7.7	Configuration field of Security mode 9	44
7.7.8	Configuration field of Security mode 10.....	46
8	Management of lower layers	48
8.1	General	48
8.2	Switching baud rate for M-Bus Link Layer according to EN 13757-2	48
8.3	Address structure if used together with the wireless Data Link Layer according to EN 13757-4.....	48
8.4	Selection and secondary addressing	48
8.5	Generalized selection procedure.....	49
8.6	Searching for installed slaves.....	50
8.6.1	Primary addresses	50
8.6.2	Secondary addresses.....	50
8.6.3	Wildcard searching procedure	50
9	Security Services	51
9.1	General	51
9.2	Message counter.....	52
9.2.1	Overview	52
9.2.2	Message counter C_M transmitted by the meter	52
9.2.3	Message counter C_{CP} transmitted by the communication partner.....	53
9.2.4	Message counter C'_{CP} received by the meter.....	53
9.2.5	Message counter C'_M and C''_M received by the communication partner	53
9.3	Authentication methods in the AFL.....	54
9.3.1	Overview	54
9.3.2	Authentication method AES-CMAC-128.....	54
9.3.3	Authentication method AES-GMAC-128	54
9.4	Encryption and Authentication methods in the TPL.....	55
9.4.1	Overview about TPL-Security mechanisms.....	55
9.4.2	Manufacturer specific Security mechanism (Security mode 1).....	57
9.4.3	Security mechanism DES-CBC (Security mode 2 and 3).....	57
9.4.4	Security mechanism AES-CBC-128 (Security mode 5).....	58
9.4.5	Security mechanism AES-CBC-128 (Security mode 7).....	59
9.4.6	Security mechanism AES-CTR-128 (Security mode 8)	59
9.4.7	Security mechanism AES-GCM-128 (Security mode 9)	61
9.4.8	Security mechanism AES-CCM-128 (Security mode 10)	64
9.5	Reaction to security failure.....	66
9.6	Key derivation.....	67
9.6.1	General	67
9.6.2	Key derivation function A.....	67
9.7	Key Exchange.....	68
Annex A (normative)	Security Information Transfer Protocol	69
A.1	Introduction.....	69
A.2	SITP Services	69
A.2.1	Transfer security information	69

A.2.2	Activate security information.....	70
A.2.3	Deactivate security information.....	70
A.2.4	Destroy security information	70
A.2.5	Combined activation/deactivation of security information.....	70
A.2.6	Generate security information.....	70
A.2.7	Get security information	70
A.2.8	Get list of all key information	70
A.2.9	Get list of active key information	70
A.2.10	Transfer end to end secured application data.....	70
A.3	CI-Fields	71
A.4	SITP structure.....	71
A.5	Block Control Field	71
A.6	Block parameters.....	72
A.7	Overview about Data Structures / Mechanisms.....	73
A.8	Data structures for Security Information.....	74
A.8.1	General.....	74
A.8.2	Data Structure 00 _h	75
A.8.3	Data Structure 01 _h	75
A.8.4	Data Structure 02 _h	75
A.8.5	Data Structure 03 _h	76
A.8.6	Data Structure 20 _h	77
A.8.7	Data Structure 21 _h	77
A.8.8	Data Structure 22 _h	78
A.9	Data structures for secured application data	79
A.9.1	General.....	79
A.9.2	Data Structure 30 _h — AES Key-Wrap	80
A.9.3	Data Structure 31 _h — HMAC-SHA256.....	81
A.9.4	Data Structure 32 _h and 33 _h — CMAC	82
A.9.5	Data Structure 34 _h — AES-GCM	82
A.9.6	Data Structure 35 _h — AES-GMAC	84
A.9.7	Data Structure 36 _h and 37 _h — AES-CCM	85
	Annex B (informative) Message counter example.....	87
	Bibliography.....	91

European foreword

This document (EN 13757-7:2018) has been prepared by Technical Committee CEN/TC 294 “Communication systems for meters”, the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by October 2018, and conflicting national standards shall be withdrawn at the latest by October 2018.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

This document together with EN 13757-3:2018 and CEN/TR 17167:2018 supersedes EN 13757-3:2013.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

The following significant technical changes have been incorporated in the new edition of this European Standard:

- new security modes (formerly “encryption mode”) 7, 8, 9 and 10 supporting encrypted and authenticated messages have been added;
- support of Key Derivation Function for the generation of ephemeral keys;
- new Authentication and Fragmentation Layer has been introduced.

EN 13757 is currently composed with the following parts:

- *Communication systems for meters — Part 1: Data exchange;*
- *Communication systems for meters — Part 2: Wired M-Bus communication;*
- *Communication systems for meters — Part 3: Application protocols;*
- *Communication systems for meters and remote reading of meters — Part 4: Wireless meter readout (Radio meter reading for operation in SRD bands);*
- *Communication systems for meters — Part 5: Wireless M-Bus relaying;*
- *Communication systems for meters — Part 6: Local Bus;*
- *Communication systems for meters — Part 7: Transport and security services;*
- *CEN/TR 17167:2018, Communication systems for meters — Accompanying TR to EN 13757-2, -3 and -7, Examples and supplementary information.*

This document falls under the Mandate EU M/441 “Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability” by providing the relevant definitions and

methods for meter data transmission on application layer level. The M/441 Mandate is driving significant development of standards in smart metering.

This document is in accordance with CEN/CLC/ETSI/TR 50572 [4].

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

This European Standard belongs to the EN 13757 series, which covers communication systems for meters. EN 13757-1 contains generic descriptions and a communication protocol. EN 13757-2 contains a physical and a Link Layer for twisted pair based Meter-Bus (M-Bus). EN 13757-3 contains detailed description of the application protocols especially the M-Bus Protocol. EN 13757-4 describes wireless communication (often called wireless M-Bus or wM-Bus). EN 13757-5 describes the wireless network used for repeating, relaying and routing for the different modes of EN 13757-4. EN 13757-6 describes a twisted pair local bus for short distance (Lo-Bus). EN 13757-7 describes transport mechanism and security methods for data. The Technical Report CEN/TR 17167 contains informative annexes from EN 13757-2, EN 13757-3 and EN 13757-7.

These upper M-Bus protocol layers can be used with various Physical Layers and with Data Link Layers and Network Layers, which support the transmission of variable length binary transparent messages. Frequently, the Physical and Link Layers of EN 13757-2 (twisted pair) and EN 13757-4 (wireless) as well as EN 13757-5 (wireless with routing function) or the alternatives described in EN 13757-1 are used. These upper M-Bus protocol layers have been optimized for minimum battery consumption of meters, especially for the case of wireless communication, to ensure long battery lifetimes of the meters. Secondly, it is optimized for minimum message length to minimize the wireless channel occupancy and hence the collision rate. Thirdly, it is optimized for minimum requirements towards the meter processor regarding requirements of RAM size, code length and computational power.

An overview of communication systems for meters is given in EN 13757-1, which also contains further definitions.

This standard concentrates on the meter communication. The meter communicates with one (or occasionally several) fixed or mobile communication partners which again might be part of a private or public network. These further communication systems might use the same or other application layer protocols, security, privacy, authentication, and management methods.

To facilitate common communication systems for CEN-meters (e.g. gas, water, thermal energy and heat cost allocators) and for electricity meters, in this standard occasionally electricity meters are mentioned. All these references are for information only and are not standard requirements. The definition of communication standards for electricity meters (possibly by a reference to CEN standards) remains solely in the responsibility of CENELEC.

NOTE 1 CEN/TR 17167:2018, Annex C specifies how parts of this standard and of EN 13757-2 and EN 13757-4 can be used to implement smart meter functionalities. Similar functionalities could also be implemented using other Physical and Link Layers.

NOTE 2 For information on installation procedures and their integration in meter management systems, see CEN/TR 17167:2018, Annex D.

The operator of a smart metering network needs to secure the network to ensure the data protection and data privacy of the consumer (see EC-Recommendation C1342 (2012)). Securing a system requires a security policy, which should address in general all constraints on functions, information flow between functions, access by external systems and threats, including software and access to data by third persons from an organizational viewpoint.

The security policy is under the responsibility of organizations according to their business processes. The major elements of a security policy, in combination with rules, will determine the overall security that is achieved. The security policy defines goals and elements of the system to be supported by organizational policy and technical implementations of security services. Establishing and executing security policies are outside the scope of this standard; however the standard provides security services supporting those policies when implemented.

A security concept refers mainly to an *architectural* model, which represents data flows between role-based data processing functions. Requirements for the security concept result from the overall security objectives in combination with the derived security services and best practice. This standard provides a set of security services allowing the design of a secure system, which is likely to resist attacks within the lifetime of the meter.

The limitation to symmetrical cipher methods for data transmission allow energy and memory efficient solutions. This is advantageous for long-term battery operated meters. It enables as well integration of unidirectional meter communication. Services like key derivation and key distribution solves the conflict between short key lifetime and long lifetime of a meter.

1 Scope

This European Standard specifies Transport and Security Services for communication systems for meters.

This European Standard specifies secure communication capabilities by design and supports the building of a secure system architecture.

This European standard is applicable to the protection of consumer data to ensure privacy.

This draft European Standard is intended to be used with the lower layer specifications determined in EN 13757-2, EN 13757-3, EN 13757-4, EN 13757-5 and EN 13757-6.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 13757-1, *Communication systems for meters - Part 1: Data exchange*

EN 13757-2, *Communication systems for meters - Part 2: Wired M-Bus communication*

EN 13757-3:2018, *Communication systems for meters — Part 3: Application protocols*

EN 13757-4:2013, *Communication systems for meters and remote reading of meters - Part 4: Wireless meter readout (Radio meter reading for operation in SRD bands)*

EN 13757-5, *Communication systems for meters - Part 5: Wireless M-Bus relaying*

EN 62056-5-3:2014, *Electricity metering data exchange - The DLMS/COSEM suite - Part 5-3: DLMS/COSEM application layer*

EN 62056-21, *Electricity metering - Data exchange for meter reading, tariff and load control - Part 21: Direct local data exchange*

ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

NIST/SP 800-38A:2001-12, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*

NIST/SP 800-38B:2005-05, *Recommendation for Block Cipher Modes of Operation: CMAC Mode for Authentication*

NIST/SP 800-38C:2004-05, *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*

NIST/SP 800-38D:2007-11, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*

NIST/SP 800-38F:2012-12, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1 application data

data used and/or generated by the metering process such as register values, tariffs, conversion factors or data used to control the metering process respectively the output or additional information

3.2 application protocol

protocol for the coding of application data

Note 1 to entry: Application protocols are specified in EN 13757-3.

3.3 authenticity

property that data originated from its purported source

[SOURCE: NIST/SP 800-38F:2012-12, NIST/SP 800-38C:2004-05]

3.4 byte

octet of bits

3.5 confidentiality

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO 7498-2:1989]

3.6 integrity data integrity

property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO 7498-2:1989]

3.7 datagram

unit of data transferred from source to destination

Note 1 to entry: In previous versions of prEN 13757-3 datagram was called telegram.

3.8 ephemeral key

key used to encrypt or decrypt a single message or for a limited time or a limited amount of data

3.9 fragment

datagram of a fragmented message

3.10**hex-ASCII**

base-16 numbers encoded as ASCII characters ('0'–'9', 'A'–'F')

[SOURCE: ANSI X9 TR-31:2010]

3.11**initialization vector**

number used as starting point for the encryption of data sequences in order to increase the security by introducing additional cryptographic variance and to synchronize cryptographic equipment

3.12**key counter**

unique counter used in the Security Information Transfer Protocol to identify a secured end to end transferred command and response

3.13**key derivation**

technique by which a (potentially large) number of keys are generated ("derived") from a single initial key and non-secret variable data with each resulting key using a non-reversible process

3.14**message**

functional set of data transferred from source to destination

Note 1 to entry: A message may consist of one or more datagrams.

3.15**message counter**

unique counter used in AFL or TPL to identify a secured message

3.16**persistent key**

cryptographic key which, needs to be kept a prolonged period

3.17**security mechanism**

mode of operation of a (symmetric) cryptographic algorithm

Note 1 to entry: The Security mechanism is identified by the Security mode.

3.18**security mode**

mode number in configuration field identifying a set of applied security mechanisms

3.19**security service**

authenticity, confidentiality and data integrity

Note 1 to entry: Security services are provided by security mechanisms.

3.20

sublayer

subdivision of a layer

[SOURCE: EN ISO/IEC 7498-1:1995]

3.21

TPL-padding

fill bytes added in TPL to fill up application data to the requested size for a block cipher

3.22

wrapper key

(symmetric) key that determines the wrapping and unwrapping functions of a wrapping mechanism

3.23

wrapping mechanism

(symmetric) key authenticated encryption mechanism that is intended for the protection of cryptographic keys and other specialized data

4 Abbreviations and symbols

4.1 Abbreviations

ACC-DMD	Access Demand
ACC-NR	Access – No Reply
ACK	Acknowledge [EN 13757-2/EN 13757-4]
AES	Advanced Encryption Standard
AFL	Authentication and Fragmentation Sublayer
APDU	Application Protocol Data Unit
APL	Application Layer
ASCII	American Standard Code for Information Interchange
BCD	Binary Coded Decimal numbers
BCF	Block control field of SITP structure, coding the usage of command or response
BID	Block identification number of SITP structure
BL	Block length of SITP structure
CBC	Cipher Block Chaining; (AES mode of operation)
CCM	Counter mode encryption algorithm with CBC-MAC (AES mode of operation)
CF	Configuration Field
CFE	Configuration Field Extension
CI	Control Information field
CMAC	Cipher-based MAC [NIST/SP 800-38B]
CNF-IR	Confirm Installation Request
CTR	Counter Mode encryption algorithm (AES mode of operation)

DES	Data Encryption Standard
DIF	Data Information Field
DLL	Data Link Layer
DLMS	Device Language Message Specification
DSI	Data structure identifier, part of block parameter structure inside SITP
DSH	Data structure header, part of block parameter structure inside SITP
DSH1	Byte one of DSH
DSH2	Byte two of DSH
ELL	Extended Link Layer
GCM	Galois/Counter Mode, an algorithm for authenticated encryption with associated data (AES mode of operation)
GMAC	a specialization of GCM for generating a message authentication code (MAC) on data that is not encrypted
ICV	Integrity check value, part of a wrapped data structure in SITP
IV	Initialization Vector
LSB	Least Significant Byte
LSBit	Least Significant Bit
MAC	Message Authentication Code
	NOTE MAC is in other standards also used as an acronym for Media Access Control for data communication at the Physical Layer.
MK	Message Key (persistent)
MLI	Message Length Indicator, part of a wrapped data structure in SITP
MSB	Most Significant Byte
MSBit	Most Significant Bit
NWL	Network Layer
OBIS	Object Identification System (EN 62056-61)
PID	Protocol identifier field, part of wrapped data structure in SITP
REQ-UD	Request User Data (class 1 or 2) [EN 13757-2/EN 13757-4]
RSP-UD	Respond User Data [EN 13757-2/EN 13757-4]
RSSI	Received Signal Strength Indicator
SITP	Security Information Transfer Protocol
SND-IR	Send Installation Request [EN 13757-4]
SND-NKE	Send Link Reset [EN 13757-2/EN 13757-4]
SND-NR	Send – No Reply [EN 13757-4]
SND-UD	Send User Data [EN 13757-2/EN 13757-4]
SND-UD2	Send User Data 2 [EN 13757-2/EN 13757-4]
SND-UD3	Send User Data 3 [EN 13757-4]

TPDU	Transport Protocol Data Unit
TPL	Transport Layer
VIF	Value Information Field
VIFE	Value Information Field Extensions

4.2 Symbols

Hexadecimal numbers are designated by a following “h”.

Binary numbers are designated by a following “b”.

Decimal numbers have no suffix.

The concatenation of fields is indicated by the symbol “||”. E. g. 12h || 34h results in 1234h.

5 Layer model

5.1 M-Bus Layers

The M-Bus covers several communication layers. The Physical Layer and the Data Link Layer are mandatory for all type of communications. The structure of these two layers depends on the communication media (wired M-Bus (EN 13757-2) and Local Bus (EN 13757-6) or wireless M-Bus (EN 13757-4 and EN 13757-5)).

The presence of the other layers depends on:

- communication media (wired/wireless M-Bus, Radio mode),
- message type (e.g. REQ-UD2 or RSP-UD),
- message length (fragmentation required),
- selected type of Security mode.

Table 1 shows the applicable layers, their order and the related part of this standard series in which they are described. The upper protocol layers AFL, TPL and APL are specified in this standard.

Table 1 — Order of M-Bus Layer

Abbreviation	Layer	Declared by CI-field	Related part of this standard series	Colour codes ^b	OSI model Layer
APL	Application Layer	a	EN 13757-1/ EN 13757-3/EN 13757	Orange	Application Presentation
TPL	Transport Layer	yes	EN 13757-7/EN 13757	Green	Session Transport
AFL	Authentication and Fragmentation Sublayer	yes	EN 13757-7	Purple	
NWL	Network Layer	yes	EN 13757-5	Pink	Network
ELL	Extended Link Layer	yes	EN 13757-4	Blue	Data Link
DLL	Data Link Layer	no	EN 13757-2/EN 13757/ EN 13757-5	Light blue	
PHY	Physical Layer	no	EN 13757-2/EN 13757/ EN 13757-5/EN 13757	Light yellow	Physical
^a The APL is not introduced by a dedicated-CI-field, but declared by CI-field of the TPL. ^b These colour codes are applied in examples given in CEN/TR 17167.					

NOTE The relation between the M-Bus Layers and the OSI Layers is not a one-to-one relation. The OSI Data Link Layer is provided by two M-Bus Layers (DLL and ELL). The functionality of the OSI Layers 4 and 5 are represented by the M-Bus Layers AFL and TPL. The functionality of the OSI Layers 6 and 7 are represented by the M-Bus Layers APL.

5.2 The CI-field principle

All layers between the DLL and the APL are introduced by a CI-field (control information field). These CI-fields declares the structure of the following layers.

The layers ELL and NWL do not provide a dedicated length information. Therefore the structure of these layers has to be derived from the CI-field. Refer to EN 13757-4 or EN 13757-5 for specification of the length of the corresponding layers and the start position of the next layer.

The AFL has a variable structure. It declares the length of this layer by a dedicated length field.

The Transport Layer and the Application Layer uses a shared CI-field. For that reason, a Transport Layer shall be present whenever the Application Layer is used in a message. The shortest Transport Layer (no header) consists of this CI-field only. The CI-field of the Transport Layer declares the used application protocol (like M-Bus Data, DLMS-Data or Alarm protocol), the origin of message (Command of Master or Slave-Response) and the fixed header structure of the TPL header. Behind this CI-field, no other CI-field follows.

The length of the APL is given by the message length reduced by the length of the other existing layers.

Table 2 — CI-field codes used by the master or the slave

CI-field	Direction	Layer	TPL-Header	Higher layer protocol
00 _h to 1F _h	Reserved for DLMS-based applications	APL	None	DLMS (see EN 13757-1)
20 _h to 4F _h	Reserved			
50 _h	Application reset or select to device	APL	None	Application Selection; according to EN 13757-3:2018, Clause 7
51 _h	Command to device (full M-Bus frame)	APL	None	M-Bus (not for wireless); according to EN 13757-3:2018, Clause 6
52 _h	Selection of device		None	Management, see 8.4
53 _h	Application reset or select to device	APL	Long	Application Selection; according to EN 13757-3:2018, Clause 7
54 _h	Request of selected application to device	APL	None	Application Selection; according to EN 13757-3:2018, Clause 7
55 _h	Request of selected application to device	APL	Long	Application Selection; according to EN 13757-3:2018, Clause 7
56 _h to 59 _h	Reserved			
5A _h	Command to device (full M-Bus frame)	APL	Short	M-Bus; according to EN 13757-3:2018, Clause 6
5B _h	Command to device (full M-Bus frame)	APL	Long	M-Bus; according to EN 13757-3:2018, Clause 6
5C _h	Synchronize action	APL	None	according to EN 13757-3:2018, Clause 12
5D _h to 5E _h	Reserved			
5F _h	Specific usage ^b	TPL	Long	NOTE See Bibliographical Entry [8].
60 _h	Command to device	APL	Long	DLMS/COSEM with OBIS-Identifier (according to EN 13757-1 and EN 62056-5-3) ^a
61 _h	Command to device	APL	Short	DLMS/COSEM with OBIS-Identifier (according to EN 13757-1 and EN 62056-5-3) ^a
62 _h to 63 _h	Reserved			
64 _h	Command to device	APL	Long	Reserved for OBIS-type value descriptors ^a
65 _h	Command to device	APL	Short	Reserved for OBIS-type value descriptors ^a
66 _h	Response of selected application from device	APL	None	Application Selection; according to EN 13757-3:2018, Clause 7
67 _h	Response of selected application from device	APL	Short	Application Selection; according to EN 13757-3:2018, Clause 7
68 _h	Response of selected application from device	APL	Long	Application Selection; according to EN 13757-3:2018, Clause 7

CI-field	Direction	Layer	TPL-Header	Higher layer protocol
69 _h	Response from device (M-Bus-Format frame)	APL	None	M-Bus; according to EN 13757-3:2018, 6, Annex G
6A _h	Response from device (M-Bus-Format frame)	APL	Short	M-Bus; according to EN 13757-3:2018, Annex G
6B _h	Response from device (M-Bus-Format frame)	APL	Long	M-Bus; according to EN 13757-3:2018, Annex G
6C _h	Time sync to device	APL	Long	According to EN 13757-3:2018, Clause 8
6D _h	Time sync to device	APL	Long	According to EN 13757-3:2018, Clause 8
6E _h	Application error from device	APL	Short	According to EN 13757-3:2018, Clause 10
6F _h	Application error from device	APL	Long	According to EN 13757-3:2018, Clause 10
70 _h	Application error from device	APL	None	According to EN 13757-3:2018, Clause 10
71 _h	Alarm from device	APL	None	According to EN 13757-3:2018, Clause 9
72 _h	Response from device (full M-Bus frame)	APL	Long	M-Bus; according to EN 13757-3:2018, Clause 6
73 _h	Response from device (M-Bus-Compact frame)	APL	Long	M-Bus; according to EN 13757-3:2018, Clause 6, Annex G
74 _h	Alarm from device	APL	Short	According to EN 13757-3:2018, Clause 9
75 _h	Alarm from device	APL	Long	According to EN 13757-3:2018, Clause 9
76 _h to 77 _h	Reserved			
78 _h	Response from device (full M-Bus frame)	APL	None	M-Bus; according to EN 13757-3:2018, Clause 6
79 _h	Response from device (M-Bus-Compact frame)	APL	None	M-Bus; according to EN 13757-3:2018, Clause 6, Annex G
7A _h	Response from device (full M-Bus frame)	APL	Short	M-Bus; according to EN 13757-3:2018, Clause 6
7B _h	Response from device (M-Bus-Compact frame)	APL	Short	M-Bus; according to EN 13757-3:2018, Annex G and EN 13757-3:2018, Clause 6
7C _h	Response from device	APL	Long	DLMS/COSEM with OBIS-Identifier (according to EN 13757-1 and EN 62056-5-3) ^a
7D _h	Response from device	APL	Short	DLMS/COSEM with OBIS-Identifier (according to EN 13757-1 and EN 62056-5-3) ^a
7E _h	Response from device	APL	Long	Reserved for OBIS-type value descriptors ^a
7F _h	Response from device	APL	Short	Reserved for OBIS-type value descriptors ^a
80 _h	Transport Layer to device (without APL)	TPL	Long	According to EN 13757-4
81 _h	Network Layer data	NWL		According to EN 13757-5

CI-field	Direction	Layer	TPL-Header	Higher layer protocol
82 _h	Network management data to device	APL	Long	According to EN 13757-4 and EN 13757-5
83 _h	Network management data to device	APL	None	According to EN 13757-4 and EN 13757-5
84 _h	Transport Layer to device (M-Bus-Compact frame expected)	TPL	Long	According to EN 13757-3:2018, Annex G
85 _h	Transport Layer to device (M-Bus-Format frame expected)	TPL	Long	According to EN 13757-3:2018, Annex G
86 _h	Reserved for Extended Link Layer	ELL		According to EN 13757-4
87 _h	Network management data from device	APL	Long	According to EN 13757-4, EN 13757-5
88 _h	Network management data from device	APL	Short	According to EN 13757-4, EN 13757-5
89 _h	Network management data from device	APL	None	According to EN 13757-4, EN 13757-5
8A _h	Transport Layer from device (without APL)	TPL	Short	According to EN 13757-4
8B _h	Transport Layer from device (without APL)	TPL	Long	According to EN 13757-4
8C _h to 8F _h	Extended Link Layer	ELL		According to EN 13757-4
90 _h	Authentication and Fragmentation Sublayer	AFL		According to Clause 6
91 _h	Reserved			
92 _h to 97 _h	Reserved			According to EN 13757-4, EN 13757-5
98 _h – 9D _h	Reserved			
9E _h	Specific usage ^b	TPL	Short	NOTE See Bibliographical Entry [8].
9F _h	Specific usage ^b	TPL	Long	NOTE See Bibliographical Entry [8].
A0 _h to B7 _h	Manufacturer specific	APL		According to EN 13757-3:2018, 13
B8 _h	Set baud rate to 300 Bd	APL	None	Management of lower layers; according to 8.2
B9 _h	Set baud rate to 600 Bd	APL	None	Management of lower layers; according to 8.2
BA _h	Set baud rate to 1 200 Bd	APL	None	Management of lower layers; according to 8.2
BB _h	Set baud rate to 2 400 Bd	APL	None	Management of lower layers; according to 8.2
BC _h	Set baud rate to 4 800 Bd	APL	None	Management of lower layers; according to 8.2

CI-field	Direction	Layer	TPL-Header	Higher layer protocol
BD _h	Set baud rate to 9 600 Bd	APL	None	Management of lower layers; according to 8.2
BE _h	Set baud rate to 19 200 Bd	APL	None	Management of lower layers; according to 8.2
BF _h	Set baud rate to 38 400 Bd	APL	None	Management of lower layers; according to 8.2
C0 _h	Command to device	APL	Long	Image transfer; according to EN 13757-3:2018, Annex I,
C1 _h	Response from device	APL	Short	Image transfer; according EN 13757-3:2018, Annex I
C2 _h	Response from device	APL	Long	Image transfer; according to EN 13757-3:2018, Annex I
C3 _h	Command to device	APL	Long	Security Information Transfer; according to Annex A
C4 _h	Response from device	APL	Short	Security Information Transfer; according to Annex A
C5 _h	Response from device	APL	Long	Security Information Transfer; according to Annex A
C6 _h to FF _h	Reserved			
NOTE All SND-UD datagrams are acknowledged in the Data Link Layer, even if the function of these CI-fields is not implemented.				
^a These application protocols also contain OBIS identifiers. In the M-Bus application protocol, these OBIS identifiers are not included, but they can be added afterwards. For generating the OBIS identifiers from M-Bus data records, EN 13757-3:2018, Annex H shall be used. ^b Used for specific national implementations. See reference in bibliography for use of this CI-field at time of release of this standard.				

6 Authentication and Fragmentation Sublayer (AFL)

6.1 Introduction

The AFL shall be considered as part of Transportation Layer. This clause explains the usage of the Authentication and Fragmentation Sublayer (AFL) in combination with the other layers and Security modes.

The Authentication and Fragmentation Sublayer provides three essential services:

- fragmentation of long messages in multiple datagrams;
- a Message Authentication Code (MAC) to prove the authenticity of the TPL and APL;
- a Message counter which supplies a security relevant message identification that may be used for the key derivation function (refer to 9.6.1).

This optional layer shall be applied if at least one of these services is required.

NOTE Message authentication codes (MAC) and Message counter can also be provided by Security mechanisms in Transport Layer.

Fragmentation is required to transport large messages, like Software update. The AFL is separated in a section for each single fragment and a section for the whole message. The position of the AFL in the M-Bus Layer Model is shown in Table 1.

In general, two alternative capabilities of message authenticity and integrity supported by MAC may be applied in AFL:

- individual fragment authentication by a MAC (this encapsulates the authentication of the fragments as layer specific protocol data units),
- overall message authentication by a MAC (this combines fragment transport with the authentication of one application protocol data unit).

The MAC service (see 9.3) protects all layers above the AFL during transmission. Therefore, no changes in higher layers are possible, as soon as the MAC has been calculated.

To ensure authentication of APDUs with other communication partners beyond media-dependant transportation, additional MAC service in Application Layer is applicable.

6.2 Overview of the AFL-Structure

A message consists of one or more fragments. Each fragment shall be transported in one Data Link Layer datagram. The shadowed fields of Table 3 are present in each fragment. The other fields are optional.

Table 3 — Overview of all AFL Fields

Size (bytes)	Field Name	Description
1	CI	Indicates that an Authentication and Fragmentation Sublayer follows.
1	AFL	AFL-Length
2	FCL	Fragmentation Control field
1	MCL	Message Control field ^a
2	KI	Key Information field ^a
4	MCR	Message counter field ^a
N ^b	MAC	Message Authentication Code ^a
2	ML	Message Length field ^a
^a This is an optional field. Their inclusion is defined by the Fragmentation Control Field specified in 6.3.2. ^b The length of MAC depends on AT-subfield in AFL.MCL.		

All multi byte fields of AFL except the AFL.MAC shall be transmitted with least significant byte first (little endian).

6.3 Components of the AFL

6.3.1 AFL Length Field (AFL.AFL)

This field describes the number of all bytes within the AFL excluding the field AFL.AFL itself.

The field AFL.AFL is not part of the MAC protected data.

6.3.2 AFL Fragmentation Control Field (AFL.FCL)

The Fragmentation Control Field indicates presence of the following fields in the current fragment.

The field AFL.FCL (see Table 4) is not part of the MAC protected data.

Table 4 — AFL Fragmentation Control Field – bit field definitions

Bit	Field Name	Description
15	RES	Reserved (0 _b by default)
14	MF	More-Fragments 0 _b This is the last fragment 1 _b More fragments are following
13	MCLP	Message Control in this Fragment Present ^a
12	MLP	Message Length in this Fragment Present ^a
11	MCRP	Message counter in this Fragment Present ^a
10	MACP	MAC in this Fragment Present ^a
9	KIP	Key Information in this Fragment Present ^a
8	RES	Reserved (0 _b by default)
7 to 0	FID	Fragment-ID
^a 0 = field is not present; 1 = field is present		

The Fragment ID is used for the identification of each single fragment of a long message. Set FID to 1 for the first fragment of a fragmented message. FID shall increment with each fragment. The FID shall never roll over. For unfragmented messages the FID shall be set to 0.

6.3.3 AFL Message Control Field (AFL.MCL)

The AFL Message Control Field indicates presence of the following fields in a fragment of the message (see Table 5).

Table 5 — AFL Message Control Field - bit field definitions

Bit	Field Name	Description
7	RES	Reserved (0 _b by default)
6	MLMP	Message Length in Message Present ^a
5	MCMP	Message counter in Message Present ^a
4	KIMP	Key Information in Message Present ^a
3	AT	Authentication-Type (see Table 6)
2		
1		
0		
^a 0 = field is not present; 1 = field is present		

The bits 4 to 7 in the AFL.MCL field define the presence of additional fields in the message.

Table 6 describes the usage of the AT-subfield.

If the AFL.MCL field is used it always shall be present in the first fragment. It shall not be present in any following fragments of the same message.

Table 6 — AT-subfield of AFL.MCL

Value	Authentication Type	Length of Authentication Code
0	No authentication	
1 to 2	Reserved	
3	AES-CMAC-128	2 bytes
4	AES-CMAC-128	4 bytes
5	AES-CMAC-128	8 bytes
6	AES-CMAC-128	12 bytes
7	AES-CMAC-128	16 bytes
8	AES-GMAC-128	12 bytes
9 to 15	Reserved	

The standard allows different levels of integrity strength e.g. by selection of Authentication tag length. The level shall be selected depending on type of application (e.g. transfer of consumption value, switch commands, software update, etc.).

6.3.4 AFL Key Information-Field (AFL.KI)

The Key Information field (see Table 7) enables the recipient of a message to identify the corresponding authentication key.

Table 7 — AFL Key Information Field - bit field definitions

Bit	Field Name	Description
15 to 8	Key Version	The Key Version identifies the applied key version, as specified in 7.7.1.
7 to 6	RES	Reserved (0 _b by default)
5 to 4	KDF-Selection	The KDF-Selection identifies the applied Key Derivation Function, as specified in Table 25.
3 to 0	Key ID	The Key ID identifies the applied key, as specified in Table 24.

In case of individual fragment authentication, the message key shall be applied for all fragments of the message. If the KI is not present, values of the configuration field in the TPL shall be used for the key selection.

6.3.5 AFL Message counter field (AFL.MCR)

Table 8 — AFL Message counter field - bit field definitions

Bits	Field Name	Description
31 to 0	C	AFL Message counter of this message. See 9.2 for details.

The presence of the filed AFL.MCR depends on the selected Security mode. See 9.4 for details.

If the Message counter Field is used, the AFL.MCR field shall always be present in the first fragment. It shall not be present in any following fragments of the same message.

If the AFL.MCR is not present, values of the Message counter field in the TPL shall be used for the AFL.MCR.

6.3.6 AFL MAC-field (AFL.MAC)

The length of the MAC field depends on the selected option in sub field AT indicated by the AFL.MCL field.

If the MAC-field is used, the AFL.MAC field shall be present in case of

- individual fragment authentication: in each fragment;
- message authentication: only in the last fragment of a message.

In deviation to the usual transmission order for multi byte fields on the M-Bus, the MSB of the MAC shall be transmitted as first byte, the LSB as last. For details of using MAC, see 9.3.

6.3.7 AFL Message Length Field (AFL.ML)

The field AFL.ML (see Table 9) declares the number of bytes following AFL.ML until the end of the unfragmented message (excluding Link Layer fields like CRC or checksum).

The message length shall be calculated before the message is separated in several fragments.

Table 9 — AFL Message Length Field - bit field definitions

Bits	Field Name	Description
15 to 0	ML	The message length allows a maximum length of 64 kBytes. The message length contains the sum of all fragments (starting from TPL) for one message. It does not include any DLL, ELL or AFL Fields.

NOTE 1 The message length is also limited by the maximum numbers of Fragment ID's (255).

NOTE 2 Not all receivers are able to receive such long messages because of the limited message buffer size.

The AFL.ML Message Length Field shall only be present in the first fragment of a fragmented message to indicate the total message length. For unfragmented messages, the field AFL.ML can be disabled.

7 Transport Layer (TPL)

7.1 Introduction

Table 10 shows a general TPL-Structure of a message with an embedded APL. Table 2 (see 5.2) shows the respective CI-fields, which introduce the TPL with one of the possible TPL-Header (marked with None, Short or Long).

Table 10 — General structure of TPL

CI-Field	TPL Header	APL data	TPL Trailer (optional)
1 byte	None header Short header Long header	Variable number	Variable number

When using a long TPL header, the meter application address is contained in this header. This meter application address may be different to the manufacturer assigned unique Link Layer Address. This allows, for example, a wired to wireless converter to supply the supported meter application address in the long data header and its own address in the radio Data Link Layer. For a simple meter, which does not need an additional converter, the short TPL header is sufficient.

If nothing other declared then multi byte fields of TPL shall be transmitted with least significant byte first (little endian).

7.2 Structure of none TPL header

This structure has no TPL header. The first byte following the CI-field is the start of the application data. This data structure does not support transmission properties like encryption, access number or an additional meter address.

This structure can be used together with the Extended Link Layer of EN 13757-4.

7.3 Structure of short TPL header

The first 4 bytes after the CI-field are always present. After the configuration field may be a configuration field extension depending on selected Security mode in the configuration field. Thereafter follows optional fields of TPL header, which depend on the Security mode, chosen in the configuration field (refer to Table 19 in 7.5.8) or from control bits of the configuration field respectively the configuration field extension (see Table 11). For details, see 7.6.

Table 11 — Short TPL header

CI-dependent fields			CF-dependent fields	
Access No.	Status	Configuration Field (CF)	Configuration Field Extension (CFE)	Optional TPL-Header Fields
1 byte	1 byte	2 bytes	0 to n bytes	0 to n bytes

The short TPL header is used for systems supporting the Physical and Link Layer of wireless M-bus communication (refer to EN 13757-4). In this standard, the Link Layer Address contains the information fields of the manufacturer, the identification number, the version and the device type. If the meter address is identical with Link Layer Address or the meter address is selected by secondary address (see 8.4), then the 8 bytes of the meter address may be omitted from the Transport Layer.

7.4 Structure of long TPL header

The first 12 bytes after the CI-field are always present. After the configuration field may be a configuration field extension depending on selected Security mode in the configuration field. Thereafter follows optional fields of TPL header, which depend on the Security mode chosen in the configuration field (refer to Table 19 in 7.5.8) or from control bits of the configuration field respectively the configuration field extension (see Table 12). For details, see 7.6.

Table 12 — Long TPL header

CI-depended fields							CF-depended fields	
Ident. No.	Manu-facturer	Version	Device type	Access No.	Status	Configuration Field (CF)	Configuration Field Extension (CFE)	Opt. TPL-Header Fields
4 bytes	2 bytes	1 byte	1 byte	1 byte	1 byte	2 bytes	0 to n bytes	0 to n bytes

The address fields of the long TPL header always contain the address of the meter regardless of the transmission direction. In case of wireless communication based on EN 13757-4, the long TPL header shall be used when the Link Layer Address differs from meter address.

7.5 CI-field dependent elements

7.5.1 Identification number

The identification number is either a fixed fabrication number or a number changeable by the customer, coded with 8 BCD packed digits (4 bytes), and which thus runs from 00000001 to 99999999. It can be

preset at fabrication time with a unique number, but can be changeable afterwards, especially if, in addition, a unique and not changeable fabrication number (see also 8.5) is provided.

An F_h at any position of Identification number shall be interpreted as wildcard. A wildcard can replace any digit with value from 0 to 9. An Identification number of e.g. 112233FF addresses all meters with Identification numbers from 11223300 to 11223399. Wildcards are used by the communication partner to address a group of meters. A meter shall accept the address with wildcards if it matches to its own address.

7.5.2 Manufacturer identification

The field manufacturer is coded unsigned binary with 2 bytes. This manufacturer ID is calculated from the ASCII code of EN 62056-21 manufacturer ID (three uppercase letters) with the following formula:

$$\begin{aligned} \text{Man. ID} = & [\text{ASCII}(\text{1st letter}) - 64] \times 32 \times 32 \\ & + [\text{ASCII}(\text{2nd letter}) - 64] \times 32 \\ & + [\text{ASCII}(\text{3rd letter}) - 64] \end{aligned} \quad (1)$$

NOTE The flag association, UK (<http://www.dlms.com/flag>) administers these three letter manufacturers ID of EN 62056-21.

An FF_h shall be interpreted as wildcard. A wildcard can replace any value from 00_h to FE_h . A Manufacturer Identification $FFFF_h$ addresses the meter independent of its own Manufacturer Identification. Wildcards are used by the communication partner to address a group of meters. A meter shall accept the address with wildcards if it matches to its own address.

7.5.3 Version identification

The field version specifies the generation or version of the device and depends on the manufacturer. It can be used to make sure that within each version number the identification number is unique.

The value FF_h shall be interpreted as a wildcard. A wildcard can replace any value from 00_h to FE_h . Wildcards are used by the communication partner to address a group of meters. A meter shall accept the address with wildcards if it matches to its own address.

7.5.4 Device type identification

The device type is coded as given in Table 13.

Table 13 — Device type identification

Device type (previously called medium)	Code bin. Bit 7 ... 0	Code hex.
Other	0000 0000	00
Oil meter	0000 0001	01
Electricity meter	0000 0010	02
Gas meter	0000 0011	03
Thermal energy meter – Heat (volume measured at return temperature: outlet)	0000 0100	04
Steam meter	0000 0101	05
Warm water meter (30 °C ... 90 °C) ^e	0000 0110	06
Water meter ^e	0000 0111	07
Heat cost allocator	0000 1000	08
Compressed air	0000 1001	09
Thermal energy meter – Cooling (volume measured at return temperature: outlet)	0000 1010	0A
Thermal energy meter – Cooling (volume measured at flow temperature: inlet)	0000 1011	0B
Thermal energy meter – Heat (volume measured at flow temperature: inlet)	0000 1100	0C
Thermal energy meter – Combined heat/cooling	0000 1101	0D
Bus/system component	0000 1110	0E
Unknown device type	0000 1111	0F
Irrigation water meter ^d	0001 0000	10
Water data logger	0001 0001	11
Gas data logger	0001 0010	12
Gas converter	0001 0011	13
Calorific value	0001 0100	14
Hot water meter (≥ 90 °C) ^d	0001 0101	15
Cold water meter ^e	0001 0110	16
Dual register (hot/cold) water meter ^{a, e}	0001 0111	17
Pressure meter	0001 1000	18
A/D converter	0001 1001	19
Smoke detector	0001 1010	1A
Room sensor (e.g. temperature or humidity)	0001 1011	1B
Gas detector	0001 1100	1C
Reserved for sensors		1D to 1F