

DIN EN 13757-7



ICS 33.200; 35.100.10; 35.100.20

Together with DIN EN
13757-3:2018-06,
supersedes
DIN EN 13757-3:2013-08

**Communication systems for meters –
Part 7: Transport and security services;
English version EN 13757-7:2018,
English translation of DIN EN 13757-7:2018-06**

Kommunikationssysteme für Zähler –
Teil 7: Transport- und Sicherheitsdienste;
Englische Fassung EN 13757-7:2018,
Englische Übersetzung von DIN EN 13757-7:2018-06

Systèmes de communication pour compteurs –
Partie 7: Services de transport et de sécurité;
Version anglaise EN 13757-7:2018,
Traduction anglaise de DIN EN 13757-7:2018-06

Document comprises 93 pages

Translation by DIN-Sprachendienst.

In case of doubt, the German-language original shall be considered authoritative.

A comma is used as the decimal marker.

Nationales Vorwort

This document (EN 13757-7:2018) has been prepared by Technical Committee CEN/TC 294 “Communication systems for meters” (Secretariat: DIN, Germany).

The responsible German body involved in its preparation was *DIN-Normenausschuss Heiz- und Raumluft-technik sowie deren Sicherheit* (DIN Standards Committee Heating and Ventilation Technology and their Safety), Working Committee NA 041-03-66 AA “Communication systems for meters (national mirror committee for CEN/TC 294)”.

Amendments

This standard differs from DIN EN 13757-3:2013-08 as follows:

- a) the new security modes (formerly “encryption mode”) 7, 8, 9 and 10, supporting encrypted and authenticated messages, have been added;
- b) a support of the key derivation function for the generation of ephemeral keys has been included;
- c) a new authentication and fragmentation layer has been introduced.

Previous editions

DIN EN 13757-3: 2005-02, 2013-08

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.AFL)	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*