This is a preview of BS EN 13757-7:2025. Click here to purchase the full version from the ANSI store.



BSI Standards Publication

Communication systems for meters

Part 7: Transport and security services

bsi.

This is a preview of BS EN 13757-7:2025. Click here to purchase the full version from the ANSI store.

National foreword

This British Standard is the UK implementation of EN 13757-7:2025. It supersedes BS EN 13757-7:2018, which is withdrawn.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 committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 26425 8

ICS 33.200; 35.100.10; 35.100.20; 91.140.50

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 30 April 2025.

Amendments/corrigenda issued since publication

Date	Text affected

This is a preview of BS EN 13757-7:2025. Click here to purchase the full version from the ANSI store.

EUROPEAN STANDARD **EN 13757-7**

NORME EUROPÉENNE

EUROPÄISCHE NORM

April 2025

ICS 33.200; 35.100.10; 35.100.20; 91.140.50 Supersedes EN 13757-7:2018

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 24 February 2025.

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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye 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

© 2025 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. EN 13757-7:2025 E

This is a preview of BS EN 13757-7:2025. Click here to purchase the full version from the ANSI store.

Contents

Page

European foreword ... 4

Introduction ... 6

1 Scope ... 8

2 Normative references ... 8

3 Terms and definitions ... 8

4 Abbreviations and symbols ... 11
4.1 Abbreviations ... 11
4.2 Symbols ... 13

5 Layer model ... 13
5.1 M-Bus Layers ... 13
5.2 The CI-field principle ... 14

6 Authentication and Fragmentation Sublayer (AFL) ... 18
6.1 Introduction ... 18
6.2 Overview of the AFL-Structure ... 19
6.3 Components of the AFL ... 20
6.3.1 AFL Length Field (AFL.AFLL) ... 20
6.3.2 AFL Fragmentation Control Field (AFL.FCL) ... 20
6.3.3 AFL Message Control Field (AFL.MCL) ... 20
6.3.4 AFL Key Information-Field (AFL.KI) ... 21
6.3.5 AFL Message counter field (AFL.MCR) ... 22
6.3.6 AFL MAC-field (AFL.MAC) ... 22
6.3.7 AFL Message Length Field (AFL.ML) ... 22

7 Transport Layer (TPL) ... 23
7.1 Introduction ... 23
7.2 Structure of none TPL header ... 23
7.3 Structure of short TPL header ... 23
7.4 Structure of long TPL header ... 24
7.5 CI-field dependent elements ... 24
7.5.1 Identification number ... 24
7.5.2 Manufacturer identification ... 25
7.5.3 Version identification ... 25
7.5.4 Device type identification ... 25
7.5.5 Access number ... 27
7.5.6 Status byte in meter messages ... 29
7.5.7 Status byte in partner messages ... 30
7.5.8 Configuration field ... 31
7.6 Configuration field dependent structure ... 32
7.6.1 General ... 32
7.6.2 Configuration field extension ... 32
7.6.3 Optional TPL-header fields ... 32
7.6.4 Optional TPL Trailer fields ... 33
7.6.5 Partial encryption ... 33
7.7 Security Mode specific TPL-fields ... 33
7.7.1 Shared subfields of configuration field and configuration field extension ... 33
7.7.2 Configuration field of Security Mode 0 ... 36

This is a preview of BS EN 13757-7:2025. Click here to purchase the full version from the ANSI store.

7.7.3 Configuration field of Security Modes 2 and 3 37
7.7.4 Configuration field of Security Mode 5 38
7.7.5 Configuration field of Security Mode 7 39
7.7.6 Configuration field of Security Mode 8 41
7.7.7 Configuration field of Security Mode 9 43
7.7.8 Configuration field of Security Mode 10 45

8 Management of lower layers 47
8.1 General 47
8.2 Switching baud rate for M-Bus Link Layer according to EN 13757-2 47
8.3 Address structure if used together with the wireless Data Link Layer according to EN 13757-4 47
8.4 Selection and secondary addressing 47
8.5 Generalized selection procedure 48
8.6 Searching for installed slaves 49
8.6.1 Primary addresses 49
8.6.2 Secondary addresses 49
8.6.3 Wildcard searching procedure 49

9 Security Services 50
9.1 General 50
9.2 Message counter 51
9.2.1 Overview 51
9.2.2 Message counter C_M transmitted by the meter 52
9.2.3 Message counter C_{CP} transmitted by the communication partner 52
9.2.4 Message counter C'_{CP} received by the meter 52
9.2.5 Message counter C'_M and C''_M received by the communication partner 53
9.3 Authentication methods in the AFL 53
9.3.1 Overview 53
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) 56
9.4.3 Security mechanism DES-CBC (Security Mode 2 and 3) 56
9.4.4 Security mechanism AES-CBC-128 (Security Mode 5) 57
9.4.5 Security mechanism AES-CBC-128 (Security Mode 7) 58
9.4.6 Security mechanism AES-CTR-128 (Security Mode 8) 59
9.4.7 Security mechanism AES-GCM-128 (Security Mode 9) 60
9.4.8 Security mechanism AES-CCM-128 (Security Mode 10) 63
9.5 Reaction to security failure 65
9.6 Key derivation 66
9.6.1 General 66
9.6.2 Key derivation function A 66
9.7 Key Exchange 67

Annex A (normative) **Security Information Transfer Protocol** 68

Annex B (informative) **Message counter example** 86

Bibliography 90

This is a preview of BS EN 13757-7:2025. Click here to purchase the full version from the ANSI store.

European foreword

This document (EN 13757-7:2025) 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 2025, and conflicting national standards shall be withdrawn at the latest by October 2025.

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 supersedes EN 13757-7:2018.

EN 13757-7:2025 includes the following significant technical changes with respect to EN 13757-7:2018:

— support of sensor devices and alarm devices;

— reduction of device types for thermal energy meter;

— support of MBAL acc. to EN 13757-8;

— introduction of a content definition for the subfield Content index in the Configuration field;

— application of a separate message counter for each Key ID used in TPL;

— update of the definition of the SITP in Annex A like adding DSI 23_h and withdrawing DSI 30_h.

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 — Part 4: Wireless M-Bus communication;*

— *Communication systems for meters — Part 5: Wireless M-Bus relaying;*

— *Communication systems for meters — Part 7: Transport and security services*;

— *Communication systems for meters — Part 8: Adaptation Layer*;

— CEN/TR 17167, *Communication systems for meters — Accompanying TR to EN 13757-2, –3 and –7, Examples and supplementary information.*

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

This document has been prepared under a standardization request addressed to CEN by the European Commission. The Standing Committee of the EFTA States subsequently approves these requests for its Member States.

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.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN website.

This is a preview of BS EN 13757-7:2025. Click here to purchase the full version from the ANSI store.

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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

This is a preview of BS EN 13757-7:2025. Click here to purchase the full version from the ANSI store.

Introduction

This document 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 13757-7 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 document 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 document 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 17167:2023, 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 17167:2023, 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 addresses 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 document; however, this document 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

This is a preview of BS EN 13757-7:2025. Click here to purchase the full version from the ANSI store.

objectives in combination with the derived security services and best practice. This document 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 integration of unidirectional meter communication as well. Services like key derivation and key distribution solves the conflict between short key lifetime and long lifetime of a meter.

This is a preview of BS EN 13757-7:2025. Click here to purchase the full version from the ANSI store.

1 Scope

This document specifies transport and security services for communication systems for meters, sensors, and actuators, used to provide metering services.

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

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

This document is intended to be used with the lower layer specifications determined in the relevant parts of the EN 13757 series.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 13757-3:2025, *Communication systems for meters — Part 3: Application protocols*

EN 13757-4:2019, *Communication systems for meters — Part 4: Wireless M-Bus communication*

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

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*

3 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp/

— IEC Electropedia: available at https://www.electropedia.org/

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.