SLOVENSKI STANDARD
oSIST prEN 13757-7:2023

01-september-2023

Komunikacijski sistemi za merilnike - 7. del: Prevoz in varnostne službe

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

Kommunikationssysteme für Zähler - Teil 7: Transport- und Sicherheitsdienste

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

Ta slovenski standard je istoveten z: prEN 13757-7

iTeh STANDARD PREVIEW
(standards.iteh.ai)
oSIST prEN 13757-7:2023
https://standards.iteh.ai/catalog/standards/sist/caebfba8-a485-4373-b382-2152d2542853/osist-pren-13757-7-2023

ICS:

33.200	Daljinsko krmiljenje, daljinske meritve (telemetrija)	Telecontrol. Telemetering
35.100.10	Fizični sloj	Physical layer
35.100.20	Podatkovni povezovalni sloj	Data link layer

oSIST prEN 13757-7:2023 en,fr,de

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

oSIST prEN 13757-7:2023
https://standards.iteh.ai/catalog/standards/sist/caebfba8-a485-4373-b382-2152d2542853/osist-pren-13757-7-2023

oSIST prEN 13757-7:2023

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 13757-7

July 2023

ICS

Will supersede 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 draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/TC 294.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CEN 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.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
oSIST prEN 13757-7:2023
https://standards.iteh.ai/catalog/standards/sist/eaebfba8-a485-4373-b382-3152d2542853/osist-pren-13757-7-2023

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

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

© 2023 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

oSIST prEN 13757-7:2023

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
oSIST prEN 13757-7:2023
https://standards.iteh.ai/catalog/standards/sist/caebfba8-a485-4373-b382-2152d2542853/osist-pren-13757-7-2023

oSIST prEN 13757-7:2023

iTeh STANDARD PREVIEW
(standards.iteh.ai)
oSIST prEN 13757-7:2023
https://standards.iteh.ai/catalog/standards/sist/caebfba8-a485-4373-b382-
2152d2542853/osist-pren-13757-7-2023

oSIST prEN 13757-7:2023

iTeh STANDARD PREVIEW
(standards.iteh.ai)
oSIST prEN 13757-7:2023
https://standards.iteh.ai/catalog/standards/sist/caebfba8-a485-4373-b382-2152d2542853/osist-pren-13757-7-2023

oSIST prEN 13757-7:2023

European foreword

This document (prEN 13757-7:2023) has been prepared by Technical Committee CEN/TC 294 “Communication systems for meters”, the secretariat of which is held by DIN.

This document is currently submitted to the CEN Enquiry.

This document will supersede EN 13757-7:2018.

This document has been prepared under a Standardization Request given to CEN by the European Commission and the European Free Trade Association, and supports essential requirements of EU Directive(s) / Regulation(s).

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.

EN 13757-7:2023 includes the following significant technical changes with respect to EN 13757-7:2018:

— support of sensor devices and alarm devices

— Reduce device types for thermal energy meter

— support of MBAL acc. to new EN 13757-8

— introduce the content definition for the subfield Content index in the Configuration field

— apply a separate message counter for each Key ID used in TPL.

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
oSIST prEN 13757-7:2023
https://standards.iteh.ai/catalog/standards/sist/caebfba8-a485-4373-b382-2152d2542853/osist-pren-13757-7-2023

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*;

— *Communication systems for meters — Part 8: Adaptation Layer*; [1]

— 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].

[1] Under development

oSIST prEN 13757-7:2023

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 13757-6 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

oSIST prEN 13757-7:2023

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[1], 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[1], 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

[1] Under development

oSIST prEN 13757-7:2023

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 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
oSIST prEN 13757-7:2023
https://standards.iteh.ai/catalog/standards/sist/caebfba8-a485-4373-b382-2152d2542853/osist-pren-13757-7-2023

oSIST prEN 13757-7:2023

1 Scope

This document specifies Transport and Security Services for communication systems for meters and remote reading of meters.

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

EN 13757-3:2023, *Communication systems for meters — Part 3: Application protocols*[1)]

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*

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
oSIST prEN 13757-7:2023
https://standards.iteh.ai/catalog/standards/sist/caebfba8-a485-4373-b382-2152d2542853/osist-pren-13757-7-2023

[1)] Under development

oSIST prEN 13757-7:2023

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.5
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

oSIST prEN 13757-7:2023
https://standards.iteh.ai/catalog/standards/sist/caebfba8-a485-4373-b382-2152d2542853/osist-pren-13757-7-2023

[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

oSIST prEN 13757-7:2023

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
oSIST prEN 13757-7:2023
https://standards.iteh.ai/catalog/standards/sist/caebfba8-a485-4373-b382-2152d2542853/osist-pren-13757-7-2023

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 for 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.

oSIST prEN 13757-7:2023

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
oSIST prEN 13757-7:2023
https://standards.iteh.ai/catalog/standards/sist/aebfba8-a485-4373-b382-2152d2542853/osist-pren-13757-7-2023

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

oSIST prEN 13757-7:2023

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.
MBAL	M-Bus Adaptation layer [prEN 13757-8]
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]

iTeh STANDARD PREVIEW
(standards.iteh.ai)
oSIST prEN 13757-7:2023
https://standards.iteh.ai/catalog/standards/sist/caebfba8-a485-4373-b382-

oSIST prEN 13757-7:2023

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)).

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

oSIST prEN 13757-7:2023
https://standards.iteh.ai/catalog/standards/sist/caebfba8-a485-4373-b382-2152d2542853/osist-pren-13757-7-2023

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.