SLOVENSKI STANDARD
oSIST prEN 13757-7:2016

01-september-2016

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**

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 13757-7:2016 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 13757-7

July 2016

ICS 33.200; 35.100.10; 35.100.20

Will supersede EN 13757-3:2013

English Version

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

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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey 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.

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. prEN 13757-7:2016 E

Contents

Page

Figures

Tables

European foreword

This document (prEN 13757-7:2016) 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 together with prEN 13757-3:2016 will supersede 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 and remote reading of meters — Part 2: Physical and link layer*;

— *Communication systems for meters and remote reading of meters — Part 3: Dedicated application layer*;

— *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* [Enquiry stage; the present document].

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].

Introduction

This draft European Standard belongs to a series of parts of EN 13757, which covers communication systems for meters and remote reading of 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). prEN 13757-7 describes transport mechanism and security methods for data.

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 meters, 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.

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 service. 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 draft European Standard specifies Transport and Security Services for communication systems for meters and remote reading of meters.

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

This draft 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 and remote reading of meters — Part 2: Physical and link layer*

prEN 13757-3:2016, *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 (IEC 62056-5-3:2013)*

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

EN 62056-61, *Electricity metering — Data exchange for meter reading, tariff and load control — Part 61: Object identification system (OBIS) (IEC 62056-61)*

ISO 8372, *Information processing — Modes of operation for a 64-bit block cipher algorithm*

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
authenticity
property that data originated from its purported source

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

3.2
byte
octet of bits

3.3
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO 7498-2:1989]

3.4
integrity
data integrity
property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO 7498-2:1989]

3.5
datagram
unit of data transferred from source to destination

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

3.6
ephemeral key
key used to encrypt or decrypt a single message or a session that is ephemeral in the system

3.7
fragment
datagram of a fragmented message

3.8
hex-ASCII
base-16 numbers encoded as ASCII characters ('0'-'9', 'A'-'F')

[SOURCE: ANSI X9 TR-31:2010]

3.9
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

3.10
key component
one of at least two parameters having the characteristics (e. g. format, randomness) of a cryptographic key that is combined with one or more like parameters to form a cryptographic key

[SOURCE: EN ISO 11568-3:1996]

3.11
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

3.12
key-encrypting key
KEK
cryptographic key that is used for the encryption or decryption of other keys

[SOURCE: NIST/SP 800-57 Part 1:2012-07]

3.13
key wrapping key
symmetric key that determines the wrapping and unwrapping functions of a key wrapping mechanism

3.14
key wrapping mechanism
symmetric key authenticated encryption mechanism that is intended for the protection of cryptographic keys and other specialized data

3.15
message
functional set of data transferred from source to destination

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

3.16
persistent key
cryptographic key which,needs to be kept a prolonged period

3.17
pseudorandom function
process that can be used to generate output from a random seed and a data variable such that the output is computationally indistinguishable from truly random output

Note 1 to entry: See NIST/SP 800–108:2009–10.

3.18
replay protection
detection of the (attempt to) replay a message at a later point in time

3.19
secure cryptographic device
device that provides secure storage for secret information such as keys and provide security services based on this secret information

[SOURCE: EN ISO 11568-3:1996]

3.20
security mechanism
mode of operation of a (symmetric) cryptographic algorithm

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

3.21
security mode
mode number in configuration field identifying a set of applied security mechanisms

3.22
security service
authenticity, confidentiality and data integrity

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

3.23
sublayer
subdivision of a layer

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

3.24
transport master key
TMK
key-encrypting key used to transfer a meter master key to the meter

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
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]
CMD	Command