ICS 17.220, 35.110, 91.140.50 SLOVENSKÁ TECHNICKÁ NORMA Máj 2018

STN	**Výmena údajov pri meraní elektrickej energie Súbor DLMS/COSEM Časť 5-3: Aplikačná vrstva DLMS/COSEM**	**STN EN 62056-5-3** 35 6131

Electricity metering data exchange - The DLMS/COSEM suite - Part 5-3: DLMS/COSEM application layer

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 04/18

Obsahuje: EN 62056-5-3:2017, IEC 62056-5-3:2017

Oznámením tejto normy sa od 14.09.2020 ruší
STN EN 62056-5-3 (35 6131) z júna 2017

126625

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 62056-5-3

November 2017

ICS 17.220; 35.110; 91.140.50

Supersedes EN 62056-5-3:2016

English Version

Electricity metering data exchange - The DLMS/COSEM suite - Part 5-3: DLMS/COSEM application layer (IEC 62056-5-3:2017)

Échange des données de comptage de l'électricité - La suite DLMS/COSEM - Partie 5-3: Couche application DLMS/COSEM
(IEC 62056-5-3:2017)

Datenkommunikation der elektrischen Energiemessung - DLMS/COSEM - Teil 5-3: DLMS/COSEM-Anwendungsschicht
(IEC 62056-5-3:2017)

This European Standard was approved by CENELEC on 2017-09-14. CENELEC 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 CENELEC 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 CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

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

Ref. No. EN 62056-5-3:2017 E

EN 62056-5-3:2017

European foreword

The text of document 13/1744/FDIS, future edition 3 of IEC 62056-5-3, prepared by IEC/TC 13 "Electrical energy measurement and control" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62056-5-3:2017.

The following dates are fixed:

• latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2018-06-14
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2020-09-14

This document supersedes EN 62056-5-3:2016.

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

Endorsement notice

The text of the International Standard IEC 62056-5-3:2017 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 61334-4-32:1996	NOTE	Harmonized as EN 61334-4-32:1996.
IEC 61334-4-511:2000	NOTE	Harmonized as EN 61334-4-511:2000.
IEC 61334-4-512:2000	NOTE	Harmonized as EN 61334-4-512:2001.
IEC 61334-5-1:2001	NOTE	Harmonized as EN 61334-5-1:2001.
IEC 62056-1-0	NOTE	Harmonized as EN 62056-1-0.
IEC 62056-6-1:2017[1)]	NOTE	Harmonized as FprEN 62056-6-1:2017.
IEC 62056-7-3:2017	NOTE	Harmonized as EN 62056-7-3:2017.
IEC 62056-7-6:2013	NOTE	Harmonized as EN 62056-7-6:2013.
IEC 62056-9-7:2013	NOTE	Harmonized as EN 62056-9-7:2013.
IEC 62056-8-5	NOTE	Harmonized as EN 62056-8-5.
IEC 62056-8-5	NOTE	Harmonized as EN 62056-8-5.

1) To be published. At draft stage.

Annex ZA
(normative)
Normative references to international publications with their corresponding European publications

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.

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

Publication	Year	Title	EN/HD	Year
IEC 61334-4-41	1996	Distribution automation using distribution line carrier systems -- Part 4: Data communication protocols -- Section 41: Application protocols - Distribution line message specification	EN 61334-4-41	1996
IEC 61334-6	2000	Distribution automation using distribution line carrier systems -- Part 6: A-XDR encoding rule	EN 61334-6	2000
IEC 62056-6-2	2017	Electricity metering data exchange - The DLMS/COSEM suite - Part 6-2: COSEM interface classes	FprEN 62056-6-2	2017
IEC 62056-8-3	2013	Electricity metering data exchange - The DLMS/COSEM suite -- Part 8-3: Communication profile for PLC S-FSK neighbourhood networks	EN 62056-8-3	2013
IEC/TR 62051	1999	Electricity metering - Glossary of terms	-	-
IEC/TR 62051-1	2004	Electricity metering - Data exchange for meter reading, tariff and load control - Glossary of terms -- Part 1: Terms related to data exchange with metering equipment using DLMS/COSEM	-	-
ISO/IEC 8824-1	-	Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation	-	-
ISO/IEC 8825-1	2015	Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)	-	-
ISO/IEC 15953	1999	Information technology - Open Systems Interconnection - Service definition for the application service object association control service element	-	-
ISO/IEC 15954	1999	Information technology - Open Systems Interconnection - Connection-mode protocol for the application service object association control service element	-	-
FIPS PUB 180-4	2012	Secure Hash Standard (SHS)	-	-
FIPS PUB 186-4	2013	Digital Signature Standard (DSS)	-	-
FIPS PUB 197	2001	Advanced Encryption Standard (AES)	-	-
ITU-T V.44	2000	Series V: Data Communication over the telephone network - Error control - Data compression procedure	-	-
ITU-T X.509	2008	Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks	-	-

EN 62056-5-3:2017

ITU-T X.693	-	Information technology - ASN.1 encoding rules: XML Encoding rules (XER)	-	-
ITU-T X.693 Corrigendum 1	-	Information technology - ASN.1 encoding rules: XML Encoding Rules (XER) Technical Corrigendum 1	-	-
ITU-T X.694	-	Information technology - ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1	-	-
ITU-T X.694 Corrigendum	-	Information technology - ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1 Technical corrigendum 1	-	-
NIST SP 800-21	2005	Guideline for Implementing Cryptography in the Federal Government	-	-
NIST SP 800-32	2001	Introduction to Public Key Technology and the Federal PKI Infrastructure	-	-
NIST SP 800-38D	-	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC	-	-
NIST SP 800-56A rev2	-	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography	-	-
NIST SP 800-57	-	Recommendation for Key Management, Part 1: General (Revision 3)	-	-
NSA1	-	Suite B Implementer's Guide to FIPS 186-3 (ECDSA)	-	-
NSA2	-	Suite B Implementer's guide to NIST SP800-56A	-	-
NSA3	-	NSA Suite B Base Certificate and CRL Profile	-	-
RFC 3394	-	Internet Engineering Task Force (IETF). Advanced Encryption Standard (AES) Key Wrap Algorithm. Edited by J. Schaad (Soaring Hawk Consulting) and R. Housley (RSA Laboratories)	-	-
RFC 5280	-	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	-	-

IEC 62056-5-3

Edition 3.0 2017-08

INTERNATIONAL STANDARD

colour inside

Electricity metering data exchange – The DLMS/COSEM suite – Part 5-3: DLMS/COSEM application layer

IEC 62056-5-3:2017-08(en)

IEC 62056-5-3

Edition 3.0 2017-08

INTERNATIONAL STANDARD

colour inside

Electricity metering data exchange – The DLMS/COSEM suite – Part 5-3: DLMS/COSEM application layer

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 17.220; 35.110; 91.140.50 ISBN 978-2-8322-4599-6

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

ELECTRICITY METERING DATA EXCHANGE – THE DLMS/COSEM SUITE –

Part 5-3: DLMS/COSEM application layer

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this International Standard may involve the use of a maintenance service concerning the stack of protocols on which the present standard IEC 62056-5-3 is based.

The IEC takes no position concerning the evidence, validity and scope of this maintenance service.

The provider of the maintenance service has assured the IEC that he is willing to provide services under reasonable and non-discriminatory terms and conditions for applicants throughout the world. In this respect, the statement of the provider of the maintenance service is registered with the IEC. Information may be obtained from:

DLMS[1] User Association
Zug/Switzerland
www.dlms.com

_____

1 Device Language Message Specification.

International Standard IEC 62056-5-3 has been prepared by IEC technical committee 13: Electrical energy measurement and control.

This third edition cancels and replaces the second edition of IEC 62056-5-3, published in 2016. It constitutes a technical revision.

The significant technical changes with respect to the previous edition are listed in Annex K (Informative).

The text of this International Standard is based on the following documents:

FDIS	Report on voting
13/1744/FDIS	13/1747/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all the parts in the IEC 62056 series, published under the general title *Electricity metering data exchange – The DLMS/COSEM suite*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This third edition of IEC 62056-5-3 has been prepared by IEC TC13 WG14 with a significant contribution of the DLMS User Association, its D-type liaison partner.

This edition is in line with DLMS UA 1000-2, the “Green Book” Ed. 8.2:2017. The main new features are the ACCESS service, the new security suites 1 and 2 supporting symmetric key and public key cryptography, the general protection mechanism and the XML schema for COSEM APDUs.

Clause 5 is based on parts of NIST documents. Reprinted courtesy of the National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce.

ELECTRICITY METERING DATA EXCHANGE – THE DLMS/COSEM SUITE –

Part 5-3: DLMS/COSEM application layer

1 Scope

This part of IEC 62056 specifies the DLMS/COSEM application layer in terms of structure, services and protocols for DLMS/COSEM clients and servers, and defines rules to specify the DLMS/COSEM communication profiles.

It defines services for establishing and releasing application associations, and data communication services for accessing the methods and attributes of COSEM interface objects, defined in IEC 62056-6-2 using either logical name (LN) or short name (SN) referencing.

Annex A (normative) defines how to use the COSEM application layer in various communication profiles. It specifies how various communication profiles can be constructed for exchanging data with metering equipment using the COSEM interface model, and what are the necessary elements to specify in each communication profile. The actual, media-specific communication profiles are specified in separate parts of the IEC 62056 series.

Annex B (normative) specifies the SMS short wrapper.

Annex C (normative) specifies the gateway protocol.

Annex D, Annex E and Annex F (informative) include encoding examples for APDUs.

Annex G (normative) provides NSA Suite B elliptic curves and domain parameters.

Annex H (informative) provides an example of an End entity signature certificate using P-256 signed with P-256.

Annex I (normative) specifies the use of key agreement schemes in DLMS/COSEM.

Annex J (informative) provides examples of exchanging protected xDLMS APDUs between a third party and a server.

Annex K (informative) lists the main technical changes in this edition of the standard.

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.

IEC 61334-4-41:1996, *Distribution automation using distribution line carrier systems – Part 4: Data communication protocols – Section 41: Application protocol – Distribution line message specification*

IEC 61334-6:2000, *Distribution automation using distribution line carrier systems – Part 6: A-XDR encoding rule*

IEC TR 62051:1999, *Electricity metering – Glossary of terms*

IEC TR 62051-1:2004, *Electricity metering – Data exchange for meter reading, tariff and load control – Glossary of terms – Part 1: Terms related to data exchange with metering equipment using DLMS/COSEM*

IEC 62056-6-2:2017, *Electricity metering data exchange – The DLMS/COSEM suite – Part 6-2: COSEM interface classes*

IEC 62056-8-3:2013, *Electricity metering data exchange – The DLMS/COSEM suite – Part 8-3: Communication profile for PLC S-FSK neighbourhood networks*

ISO/IEC 8824-1, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*

ISO/IEC 8825-1:2015, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO/IEC 15953:1999, *Information technology – Open Systems Interconnection – Service definition for the Application Service Object Association Control Service Element*

NOTE This standard cancels and replaces ISO/IEC 8649:1996 and its Amd. 1:1997 and Amd. 2:1998, of which it constitutes a technical revision.

ISO/IEC 15954:1999, *Information technology – Open Systems Interconnection – Connection-mode protocol for the Application Service Object Association Control Service Element*

NOTE This standard cancels and replaces ISO/IEC 8650-1:1999 and its Amd. 1:1997 and Amd. 2:1998, of which it constitutes a technical revision.

ITU-T V.44: 2000 , *Series v: data communication over the telephone network – Error control – V.44:2000, Data compression procedures*

ITU-T X.509:2008, *Series x: data networks, open system communications and security – Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*

ITU-T X.693 (11/2008), *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER)*

ITU-T X.693 Corrigendum 1 (10/2011), *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER) Technical Corrigendum 1*

ITU-T X.694 (11/2008), *Information technology – ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1*

ITU-T X.694 Corrigendum 1 (10/2011), *Information technology – ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1 Technical Corrigendum 1*

FIPS PUB 180-4:2012, *Secure hash standard (SHS)*

FIPS PUB 186-4:2013, *Digital Signature Standard (DSS)*

FIPS PUB 197:2001, *Advanced Encryption Standard (AES)*

NIST SP 800-21:2005, *Guideline for Implementing Cryptography in the Federal Government*

NIST SP 800-32:2001, *Introduction to Public Key Technology and the Federal PKI Infrastructure*

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

NIST SP 800-56A Rev. 2: 2013, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*

NIST SP 800-57:2012, *Recommendation for Key Management – Part 1: General (Revision 3)*

NSA1, *Suite B Implementer's Guide to FIPS 186-3 (ECDSA)*, Feb 3rd 2010

NSA2, *Suite B Implementer's Guide to NIST SP800-56A*, 28th July 2009

NSA3, *NSA Suite B Base Certificate and CRL Profile*, 27th May 2008

RFC 3394, *Advanced Encryption Standard (AES) Key Wrap Algorithm*. Edited by J. Schaad (Soaring Hawk Consulting) and R. Housley (RSA Laboratories) September 2002 http://tools.ietf.org/html/rfc3394

RFC 4108, *Using Cryptographic Message Syntax (CMS) to Protect Firmware Packages*, 2005, http://www.ietf.org/rfc/rfc4108

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, 2008, http://www.ietf.org/rfc/rfc5280