

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

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 62056-5-3:2016 sisaldab Euroopa standardi EN 62056-5-3:2016 ingliskeelset teksti.	This Estonian standard EVS-EN 62056-5-3:2016 consists of the English text of the European standard EN 62056-5-3:2016.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 09.12.2016.	Date of Availability of the European standard is 09.12.2016.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 17.220, 35.110, 91.140.50

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:
Koduleht www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation:

Homepage www.evs.ee; phone +372 605 5050; e-mail info@evs.ee

English Version

**Electricity metering data exchange - The DLMS/COSEM suite -
Part 5-3: DLMS/COSEM application layer
(IEC 62056-5-3:2016)**

Échange des données de comptage de l'électricité - La
suite DLMS/COSEM - Partie 5-3: Couche application
DLMS/COSEM
(IEC 62056-5-3:2016)

Datenkommunikation der elektrischen Energiemessung -
DLMS/COSEM - Teil 5-3: DLMS/COSEM-
Anwendungsschicht
(IEC 62056-5-3:2016)

This European Standard was approved by CENELEC on 2016-04-08. 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, 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

European foreword

The text of document 13/1648/FDIS, future edition 2 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 62056-5-3:2016.

The following dates are fixed:

- latest date by which the document has to be (dop) 2017-06-09
implemented at national level by
publication of an identical national
standard or by endorsement
- latest date by which the national (dow) 2019-12-09
standards conflicting with the
document have to be withdrawn

This document supersedes EN 62056-5-3:2014.

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

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association.

Endorsement notice

The text of the International Standard IEC 62056-5-3:2016 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 61334-4-3:1996	NOTE	Harmonized as EN 61334-4-32:1996 (not modified).
IEC 61334-4-511:2000	NOTE	Harmonized as EN 61334-4-511:2000 (not modified).
IEC 61334-4-512:2001	NOTE	Harmonized as EN 61334-4-512:2002 (not modified).
IEC 61334-5-1:2001	NOTE	Harmonized as EN 61334-5-1:2001 (not modified).
IEC 62056-7-6:2013	NOTE	Harmonized as EN 62056-7-6:2013 (not modified).
IEC 62056-9-7:2013	NOTE	Harmonized as EN 62056-9-7:2013 (not modified).
ISO/IEC 7498-1:1994	NOTE	Harmonized as EN ISO/IEC 7498-1:1994 ¹⁾ (not modified).

¹⁾ Withdrawn publication.

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

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.

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

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
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/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 62056-1-0	-	Electricity metering data exchange - The DLMS/COSEM suite - Part 1-0: Smart metering standardisation framework	EN 62056-1-0	-
IEC 62056-6-1	2015	Electricity metering data exchange - The DLMS/COSEM suite - Part 6-1: Object Identification System (OBIS)	EN 62056-6-1	2016
IEC 62056-6-2	2016	Electricity metering data exchange - The DLMS/COSEM suite - Part 6-2: COSEM interface classes	EN 62056-6-2	2016
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
ISO/IEC 8824-1	2008 ²⁾	Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation	-	-

²⁾ Superseded by ISO/IEC 8824-1:2015.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
ISO/IEC 8825-1	2008 ³⁾	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 197	2001	Advanced Encryption Standard (AES)	-	-
NIST SP 800-38D	2007	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC	-	-
NIST SP 800-57	2007	Recommendation for key management - Part 1: General	-	-
RFC 1321	1992	The MD5 Message-Digest Algorithm. Edited by R. Rivest (MIT Laboratory for Computer Science and RSA Data Security, Inc.)	-	-
RFC 3394	2002	Advanced Encryption Standard (AES) Key Wrap Algorithm. Edited by J. Schaad (Soaring Hawk Consulting) and R. Housley (RSA Laboratories)	-	-
RFC 4106	-	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)	-	-

³⁾ Superseded by ISO/IEC 8825-1:2015.

CONTENTS

FOREWORD.....	8
INTRODUCTION.....	10
1 Scope.....	11
2 Normative references	11
3 Terms, definitions and abbreviations	13
3.1 Terms and definitions	13
3.2 Abbreviations	13
4 Overview	15
4.1 DLMS/COSEM application layer structure	15
4.2 DLMS/COSEM application layer services	16
4.2.1 ASO services	16
4.2.2 Services provided for application association establishment and release	16
4.2.3 Services provided for data transfer	17
4.2.4 Layer management services	22
4.2.5 Summary of DLMS/COSEM application layer services	22
4.3 DLMS/COSEM application layer protocols	22
5 Information security in DLMS/COSEM	23
5.1 Definitions	23
5.2 General.....	23
5.3 Data access security	24
5.3.1 Overview	24
5.3.2 No security (lowest level security) authentication	24
5.3.3 Low Level Security (LLS) authentication	24
5.3.4 High Level Security (HLS) authentication.....	25
5.4 Data transport security	27
5.4.1 Applying, removing or checking the protection: ciphering and deciphering.....	27
5.4.2 Security context	28
5.4.3 Security policy	28
5.4.4 Security suite	29
5.4.5 Security material	29
5.4.6 Ciphered xDLMS APDUs	29
5.4.7 Cryptographic keys	31
5.4.8 The Galois/Counter Mode of Operation (GCM).....	34
6 DLMS/COSEM application layer service specification	43
6.1 Service primitives and parameters	43
6.2 The COSEM-OPEN service	45
6.3 The COSEM-RELEASE service	50
6.4 COSEM-ABORT service	52
6.5 Protection and general block transfer parameters	53
6.6 The GET service	57
6.7 The SET service	59
6.8 The ACTION service	62
6.9 The DataNotification service	66
6.10 The EventNotification service	67
6.11 The TriggerEventNotificationSending service	68

6.12	Variable access specification.....	69
6.13	The Read service.....	69
6.14	The Write service.....	73
6.15	The UnconfirmedWrite service.....	76
6.16	The InformationReport service.....	77
6.17	Client side layer management services: the SetMapperTable.request.....	78
6.18	Summary of services and LN/SN data transfer service mapping	78
7	DLMS/COSEM application layer protocol specification.....	79
7.1	The control function	79
7.1.1	State definitions of the client side control function.....	79
7.1.2	State definitions of the server side control function	81
7.2	The ACSE services and APDUs.....	82
7.2.1	ACSE functional units, services and service parameters	82
7.2.2	Registered COSEM names.....	85
7.2.3	APDU encoding rules	87
7.2.4	Protocol for application association establishment	87
7.2.5	Protocol for application association release	92
7.3	Protocol for the data transfer services	95
7.3.1	Negotiation of services and options – the conformance block.....	95
7.3.2	Confirmed and unconfirmed service invocations.....	96
7.3.3	Protocol for the GET service	98
7.3.4	Protocol for the SET service.....	101
7.3.5	Protocol for the ACTION service.....	104
7.3.6	Protocol of the DataNotification service	106
7.3.7	Protocol for the EventNotification service.....	106
7.3.8	Protocol for the Read service	106
7.3.9	Protocol for the Write service	110
7.3.10	Protocol for the UnconfirmedWrite service.....	114
7.3.11	Protocol for the InformationReport service.....	115
7.3.12	Protocol of general block transfer mechanism.....	116
8	Abstract syntax of ACSE and COSEM APDUs	127
Annex A (normative) Using the COSEM application layer in various communications profiles		142
A.1	General.....	142
A.2	Targeted communication environments.....	142
A.3	The structure of the profile	142
A.4	Identification and addressing schemes	142
A.5	Supporting layer services and service mapping.....	143
A.6	Communication profile specific parameters of the COSEM AL services.....	143
A.7	Specific considerations / constraints using certain services within a given profile	143
A.8	The 3-layer, connection-oriented, HDLC based communication profile.....	143
A.9	The TCP-UDP/IP based communication profiles (COSEM_on_IP)	143
A.10	The S-FSK PLC profile	143
Annex B (normative) SMS short wrapper		144
Annex C (informative) AARQ and AARE encoding examples		145
C.1	General.....	145
C.2	Encoding of the xDLMS InitiateRequest / InitiateResponse APDUs.....	145
C.3	Specification of the AARQ and AARE APDUs	148

C.4	Data for the examples	149
C.5	Encoding of the AARQ APDU	150
C.6	Encoding of the AARE APDU.....	153
Annex D (informative) Encoding examples: AARQ and AARE APDUs using a ciphered application context.....		159
D.1	A-XDR encoding of the xDLMS InitiateRequest APDU, carrying a dedicated key	159
D.2	Authenticated encryption of the xDLMS InitiateRequest APDU	160
D.3	The AARQ APDU	161
D.4	A-XDR encoding of the xDLMS InitiateResponse APDU	162
D.5	Authenticated encryption of the xDLMS InitiateResponse APDU.....	163
D.6	The AARE APDU.....	164
D.7	The RLRQ APDU (carrying a ciphered xDLMS InitiateRequest APDU).....	165
D.8	The RLRE APDU (carrying a ciphered xDLMS InitiateResponse APDU).....	166
Annex E (informative) Data transfer service examples		167
Annex F (informative) Overview of cryptography		183
F.1	General.....	183
F.2	Hash functions	183
F.3	Symmetric key algorithms.....	184
F.3.1	General	184
F.3.2	Encryption and decryption	184
F.3.3	Advanced Encryption Standard (AES).....	185
F.3.4	Encryption Modes of Operation	185
F.3.5	Message Authentication Code	186
F.3.6	Key establishment.....	187
F.4	Asymmetric key algorithms	187
F.4.1	General	187
F.4.2	Digital signatures	188
F.4.3	Key establishment.....	188
Annex G (informative) Significant technical changes with respect to IEC 62056-5-3 Ed.1.0:2013		189
Bibliography		191
Index.....		194
Figure 1 – Structure of the COSEM Application layers		15
Figure 2 – Summary of DLMS/COSEM AL services.....		22
Figure 3 – Authentication mechanisms during AA establishment		27
Figure 4 – Structure of service specific global ciphering and dedicated ciphering APDUs		30
Figure 5 – Structure of general global ciphering and dedicated ciphering APDUs		30
Figure 6 – Cryptographic protection of xDLMS APDUs using GCM		37
Figure 7 – Service primitives		43
Figure 8 – Time sequence diagrams.....		44
Figure 9 – Additional service parameters to control cryptographic protection and general block transfer		54
Figure 10 – Partial state machine for the client side control function		80
Figure 11 – Partial state machine for the server side control function		81

Figure 12 – MSC for successful AA establishment preceded by a successful lower layer connection establishment	88
Figure 13 – Graceful AA release using the A-RELEASE service	93
Figure 14 – Graceful AA release by disconnecting the supporting layer	94
Figure 15 – Aborting an AA following a PH-ABORT.indication	95
Figure 16 – MSC of the GET service	98
Figure 17 – MSC of the GET service with block transfer.....	99
Figure 18 – MSC of the GET service with block transfer, long GET aborted.....	101
Figure 19 – MSC of the SET service.....	102
Figure 20 – MSC of the SET service with block transfer	102
Figure 21 – MSC of the ACTION service	104
Figure 22 – MSC of the ACTION service with block transfer.....	105
Figure 23 – MSC of the Read service used for reading an attribute	109
Figure 24 – MSC of the Read service used for invoking a method	109
Figure 25 – MSC of the Read Service used for reading an attribute, with block transfer.....	110
Figure 26 – MSC of the Write service used for writing an attribute.....	113
Figure 27 – MSC of the Write service used for invoking a method	113
Figure 28 – MSC of the Write service used for writing an attribute, with block transfer.....	114
Figure 29 – MSC of the Unconfirmed Write service used for writing an attribute	115
Figure 30 – Partial service invocations and GBT APDUs.....	118
Figure 31 – GET service with GBT, switching to streaming	120
Figure 32 – GET service with partial invocations, GBT and streaming, recovery of 4 th block sent in the 2nd stream	121
Figure 33 – GET service with partial invocations, GBT and streaming, recovery of 4 th and 5 th blocks	122
Figure 34 – GET service with partial invocations, GBT and streaming, recovery of last block	123
Figure 35 – SET service with GBT, with server not supporting streaming, recovery of 3rd block	124
Figure 36 – ACTION-WITH-LIST service with bi-directional GBT and block recovery	125
Figure 37 – DataNotification service with GBT with partial invocation	126
Figure B.1 – Short wrapper	144
Figure F.1 – Hash function	184
Figure F.2 – Encryption and decryption	185
Figure F.3 – Message Authentication Codes (MACs)	186
Table 1 – Clarification of the meaning of PDU Size for DLMS/COSEM	18
Table 2 – Security suites.....	29
Table 3 – Ciphered xDLMS APDUs	29
Table 4 – Use of the fields of the ciphered APDUs.....	31
Table 5 – Cryptographic keys and their management.....	34
Table 6 – Security control byte	38
Table 7 – Plaintext and additional authenticated data	38
Table 8 – Example for ciphered APDUs.....	40
Table 9 – HLS example with GMAC.....	42

Table 10 – Codes for AL service parameters	45
Table 11 – Service parameters of the COSEM-OPEN service primitives	46
Table 12 – Service parameters of the COSEM-RELEASE service primitives	50
Table 13 – Service parameters of the COSEM-ABORT service primitives	53
Table 14 – Additional service parameters	55
Table 15 – Security parameters	56
Table 16 – Service parameters of the GET service	57
Table 17 – GET service request and response types	58
Table 18 – Service parameters of the SET service	60
Table 19 – SET service request and response types	61
Table 20 – Service parameters of the ACTION service	63
Table 21 – ACTION service request and response types	64
Table 22 – Service parameters of the DataNotification service primitives	66
Table 23 – Service parameters of the EventNotification service primitives	67
Table 24 – Service parameters of the TriggerEventNotificationSending.request service primitive	68
Table 25 – Variable Access Specification	69
Table 26 – Service parameters of the Read service	70
Table 27 – Use of the Variable_Access_Specification variants and the Read.response choices	71
Table 28 – Service parameters of the Write service	74
Table 29 – Use of the Variable_Access_Specification variants and the Write.response choices	74
Table 30 – Service parameters of the UnconfirmedWrite service	76
Table 31 – Use of the Variable_Access_Specification variants	77
Table 32 – Service parameters of the InformationReport service	78
Table 33 – Service parameters of the SetMapperTable.request service primitives	78
Table 34 – Summary of ACSE services	79
Table 35 – Summary of xDLMS services for LN referencing	79
Table 36 – Summary of xDLMS services for SN referencing	79
Table 37 – ACSE functional units, services and service parameters	83
Table 38 – Use of ciphered / unciphered APDUs	86
Table 39 – xDLMS Conformance block	96
Table 40 – GET service types and APDUs	98
Table 41 – SET service types and APDUs	101
Table 42 – ACTION service types and APDUs	104
Table 43 – Mapping between the GET and the Read services	107
Table 44 – Mapping between the ACTION and the Read services	108
Table 45 – Mapping between the SET and the Write services	111
Table 46 – Mapping between the ACTION and the Write service	112
Table 47 – Mapping between the SET and the UnconfirmedWrite services	115
Table 48 – Mapping between the ACTION and the UnconfirmedWrite services	115
Table 49 – Mapping between the EventNotification and InformationReport services	116
Table B.1 – Reserved Application Processes	144

Table C.1 – Conformance block	146
Table C.2 – A-XDR encoding of the xDLMS InitiateRequest APDU	147
Table C.3 – A-XDR encoding of the xDLMS InitiateResponse APDU	148
Table C.4 – BER encoding of the AARQ APDU	151
Table C.5 – Complete AARQ APDU	153
Table C.6 – BER encoding of the AARE APDU	154
Table C.7 – The complete AARE APDU	158
Table D.1 – A-XDR encoding of the xDLMS InitiateRequest APDU	159
Table D.2 – Authenticated encryption of the xDLMS InitiateRequest APDU	160
Table D.3 – BER encoding of the AARQ APDU	161
Table D.4 – A-XDR encoding of the xDLMS InitiateResponse APDU	163
Table D.5 – Authenticated encryption of the xDLMS InitiateResponse APDU	163
Table D.6 – BER encoding of the AARE APDU	164
Table D.7 – BER encoding of the RLRQ APDU	166
Table D.8 – BER encoding of the RLRE APDU	166
Table E.1 – Objects used in the examples	167
Table E.2 – Example: Reading the value of a single attribute without block transfer	168
Table E.3 – Example: Reading the value of a list of attributes without block transfer	169
Table E.4 – Example: Reading the value of a single attribute with block transfer	171
Table E.5 – Example: Reading the value of a list of attributes with block transfer	173
Table E.6 – Example: Writing the value of a single attribute without block transfer	176
Table E.7 – Example: Writing the value of a list of attributes without block transfer	177
Table E.8 – Example: Writing the value of a single attribute with block transfer	178
Table E.9 – Example: Writing the value of a list of attributes with block transfer	180

INTRODUCTION

This second 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 the DLMS UA Green Book Edition 7.0 Amendment 3. The main new features are the DataNotification service, the general protection and the general block transfer mechanisms and the SMS short wrapper.

In 2014, the DLMS UA has published Green Book Edition 8.0 adding several new features regarding functionality, efficiency and security while keeping full backwards compatibility.

The intention of the DLMS UA is to bring also these latest developments to international standardization. Therefore, IEC TC13 WG14 launched a project to bring these new elements also to the IEC 62056 series that will lead to Edition 3.0 of the standard.

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