

© Copyright SEK. Reproduction in any form without permission is prohibited.

Elmätare – Datakommunikation för avläsning av elmätare och för styrning av tariff och belastning – Del 5-3: Tillämpningsskikt COSEM

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

Som svensk standard gäller europastandarden EN 62056-5-3:2014. Den svenska standarden innehåller den officiella engelska språkversionen av EN 62056-5-3:2014.

Nationellt förord

Europastandarden EN 62056-5-3:2014

består av:

- **europastandardens ikraftsättningsdokument**, utarbetat inom CENELEC
- **IEC 62056-5-3, First edition, 2013 - Electricity metering data exchange - The DLMS/COSEM suite - Part 5-3: DLMS/COSEM application layer**

utarbetad inom International Electrotechnical Commission, IEC.

Tidigare fastställd svensk standard SS-EN 62056-53, utgåva 2, 2007, gäller ej fr o m 2016-07-10.

Standardern ersätter delvis SS-EN 62056-53, utgåva 2, 2007.

ICS 17.220.00; 35.110.00; 91.140.50

Denna standard är fastställd av SEK Svensk Elstandard,
som också kan lämna upplysningar om **sakinnehållet** i standarden.
Postadress: Box 1284, 164 29 KISTA
Telefon: 08 - 444 14 00.
E-post: sek@elstandard.se. Internet: www.elstandard.se

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a säkerhet, prestanda, dokumentation, utförande och skötsel av elprodukter, elanläggningar och metoder. Genom att utforma sådana standarder blir säkerhetskraven tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard

Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se

**Electricity metering data exchange -
The DLMS/COSEM suite -
Part 5-3: DLMS/COSEM application layer
(IEC 62056-5-3:2013)**

Échange des données de comptage de
l'électricité -
La suite DLMS/COSEM -
Partie 5-3: Couche application
DLMS/COSEM
(CEI 62056-5-3:2013)

Datenkommunikation der elektrischen
Energienmessung - DLMS/COSEM -
Teil 5-3: DLMS/COSEM-
Anwendungsschicht
(IEC 62056-5-3:2013)

This European Standard was approved by CENELEC on 2013-07-10. 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.

CENELEC

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

Foreword

The text of document 13/1523/FDIS, future edition 1 of IEC 62056-5-3, prepared by IEC/TC 13 "Electrical energy measurement, tariff- and load control" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62056-5-3:2014.

The following dates are fixed:

- latest date by which the document has to be (dop) 2014-09-07
implemented at national level by
publication of an identical national
standard or by endorsement
- latest date by which the national (dow) 2016-07-10
standards conflicting with the
document have to be withdrawn

This document supersedes EN 62056-53:2007 (PART).

EN 62056-5-3:2014 includes the following significant technical changes with respect to EN 62056-53:2007:

The significant technical changes with respect to EN 62056-53 are listed in Annex F.

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.

Endorsement notice

The text of the International Standard IEC 62056-5-3:2013 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 (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 62056-1-0 ¹⁾	NOTE	Harmonized as EN 62056-1-0 ¹⁾ .
ISO/IEC 7498-1:1994	NOTE	Harmonized as EN ISO/IEC 7498-1:1995 ²⁾ (not modified).

¹⁾ At draft stage.

²⁾ 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 When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

<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 + corr. June	2004 2005	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 62056-6-1	2013	Electricity metering data exchange - The DLMS/COSEM suite - Part 6-1: COSEM Object Identification System (OBIS)	EN 62056-6-1	2013
IEC 62056-6-2	2013	Electricity metering data exchange - The DLMS/COSEM suite - Part 6-2: COSEM interface classes	EN 62056-6-2	2013
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 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	-	-
ISO/IEC 8824-1	2008	Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation	-	-
ISO/IEC 8825-1	2008	Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)	-	-

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
FIPS PUB 180-1	1995 ³⁾	Secure hash standard	-	-
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 ⁴⁾	Recommendation for key management - Part 1: General	-	-
RFC 1321	1992	Internet Engineering Task Force (IETF). The MD5 Message-Digest Algorithm. Edited by R. Rivest (MIT Laboratory for Computer Science and RSA Data Security, Inc.)	-	-
RFC 3394	2002	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 4106	2005	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)	-	-

³⁾ Superseded by FIPS PUB 180-2:2002, which is also superseded by FIPS PUB 180-4:2012.

⁴⁾ Superseded by NIST SP 800-57:2012.

CONTENTS

1	Scope	9
2	Normative references	9
3	Terms, definitions and abbreviations	11
3.1	Terms and definitions	11
3.2	Abbreviations	11
4	Overview	13
4.1	COSEM application layer structure	13
4.2	COSEM application layer services	14
4.2.1	ASO services	14
4.2.2	Services provided for application association establishment and release	14
4.2.3	Services provided for data transfer	15
4.2.4	Layer management services	19
4.2.5	Summary of COSEM application layer services	19
4.3	COSEM application layer protocols	20
5	Information security in DLMS/COSEM	20
5.1	Definitions	20
5.2	General	20
5.3	Data access security	21
5.3.1	Overview	21
5.3.2	Lowest level security (no security)	21
5.3.3	Low Level Security (LLS)	21
5.3.4	High Level Security (HLS)	22
5.4	Data transport security	23
5.4.1	Applying, removing or checking the protection: ciphering and deciphering	23
5.4.2	Security context	25
5.4.3	Security policy	25
5.4.4	Security suite	25
5.4.5	Security material	26
5.4.6	Ciphered xDLMS APDUs	26
5.4.7	Cryptographic keys	27
5.4.8	The Galois/Counter Mode of Operation (GCM)	30
6	COSEM application layer service specification	40
6.1	Service primitives and parameters	40
6.2	The COSEM-OPEN service	42
6.3	The COSEM-RELEASE service	47
6.4	COSEM-ABORT service	49
6.5	Security parameters	50
6.6	The GET service	51
6.7	The SET service	53
6.8	The ACTION service	56
6.9	The EventNotification service	60
6.10	The TriggerEventNotificationSending service	61
6.11	Variable access specification	62
6.12	The Read service	63

6.13	The Write service	67
6.14	The UnconfirmedWrite service.....	70
6.15	The InformationReport service.....	71
6.16	Client side layer management services: the SetMapperTable.request.....	72
6.17	Summary of services and LN/SN data transfer service mapping	72
7	COSEM application layer protocol specification	73
7.1	The control function.....	73
7.1.1	State definitions of the client side control function	73
7.1.2	State definitions of the server side control function	75
7.2	The ACSE services and APDUs	76
7.2.1	ACSE functional units, services and service parameters.....	76
7.2.2	Registered COSEM names	79
7.2.3	APDU encoding rules	81
7.2.4	Protocol for application association establishment.....	81
7.2.5	Protocol for application association release	85
7.3	Protocol for the data transfer services	89
7.3.1	Negotiation of services and options – the conformance block	89
7.3.2	Confirmed and unconfirmed service invocations	90
7.3.3	Protocol for the GET service.....	91
7.3.4	Protocol for the SET service	94
7.3.5	Protocol for the ACTION service.....	97
7.3.6	Protocol for the EventNotification service	99
7.3.7	Protocol for the Read service	100
7.3.8	Protocol for the Write service.....	104
7.3.9	Protocol for the UnconfirmedWrite service	108
7.3.10	Protocol for the InformationReport service	109
8	Abstract syntax of ACSE and COSEM APDUs	110
Annex A (normative)	Using the COSEM application layer in various communications profiles	124
Annex B (informative)	AARQ and AARE encoding examples.....	126
Annex C (informative)	Encoding examples: AARQ and AARE APDUs using a ciphered application context.....	140
Annex D (informative)	Data transfer service examples	148
Annex E (informative)	Overview of cryptography	163
Annex F (informative)	Significant technical changes with respect to IEC 62056-53	169
Bibliography		172
Index		174
Figure 1	– Structure of the COSEM Application layers	13
Figure 2	– Summary of COSEM AL services	19
Figure 3	– LLS and HLS authentication	23
Figure 4	– Data transport security in DLMS/COSEM	24
Figure 5	– Ciphered xDLMS APDUs.....	26
Figure 6	– Cryptographic protection of xDLMS APDUs using GCM.....	33
Figure 7	– Service primitives.....	40
Figure 8	– Time sequence diagrams	41
Figure 9	– Partial state machine for the client side control function	74

Figure 10 – Partial state machine for the server side control function.....	75
Figure 11 – MSC for successful AA establishment preceded by a successful lower layer connection establishment	82
Figure 12 – Graceful AA release using the A-RELEASE service.....	87
Figure 13 – Graceful AA release by disconnecting the supporting layer	88
Figure 14 – Aborting an AA following a PH-ABORT.indication	89
Figure 15 – MSC of the GET service.....	92
Figure 16 – MSC of the GET service with block transfer	92
Figure 17 – MSC of the GET service with block transfer, long GET aborted	94
Figure 18 – MSC of the SET service	95
Figure 19 – MSC of the SET service with block transfer	96
Figure 20 – MSC of the ACTION service.....	98
Figure 21 – MSC of the ACTION service with block transfer.....	99
Figure 22 – MSC of the Read service used for reading an attribute.....	102
Figure 23 – MSC of the Read service used for invoking a method.....	103
Figure 24 – MSC of the Read Service used for reading an attribute, with block transfer	104
Figure 25 – MSC of the Write service used for writing an attribute	107
Figure 26 – MSC of the Write service used for invoking a method.....	107
Figure 27 – MSC of the Write Service used for writing an attribute, with block transfer	108
Figure 28 – MSC of the Unconfirmed Write service used for writing an attribute.....	109
Figure E.1 – Hash function.....	164
Figure E.2 – Encryption and decryption.....	165
Figure E.3 – Message Authentication Codes (MACs)	166
Table 1 – Clarification of the meaning of PDU Size for DLMS/COSEM	16
Table 2 – Security suites	26
Table 3 – Security control field.....	27
Table 4 – Cryptographic keys and their management.....	30
Table 5 – Plaintext and additional authenticated data	34
Table 6 – Example for ciphered APDUs	37
Table 7 – HLS example with GMAC	39
Table 8 – Codes for AL service parameters	42
Table 9 – Service parameters of the COSEM-OPEN service primitives	43
Table 10 – Service parameters of the COSEM-RELEASE service primitives	47
Table 11 – Service parameters of the COSEM-ABORT service primitives	50
Table 12 – Security parameters	50
Table 13 – Service parameters of the GET service	51
Table 14 – GET service request and response types	52
Table 15 – Service parameters of the SET service.....	54
Table 16 – SET service request and response types.....	55
Table 17 – Service parameters of the ACTION service	57
Table 18 – ACTION service request and response types	58
Table 19 – Service parameters of the EventNotification service primitives	60

Table 20 – Service parameters of the TriggerEventNotificationSending.request service primitive	61
Table 21 – Variable Access Specification	63
Table 22 – Service parameters of the Read service	64
Table 23 – Use of the Variable_Access_Specification variants and the Read.response choices	65
Table 24 – Service parameters of the Write service	68
Table 25 – Use of the Variable_Access_Specification variants and the Write.response choices	68
Table 26 – Service parameters of the UnconfirmedWrite service	70
Table 27 – Use of the Variable_Access_Specification variants	71
Table 28 – Service parameters of the InformationReport service	72
Table 29 – Service parameters of the SetMapperTable.request service primitives	72
Table 30 – Summary of ACSE services	73
Table 31 – Summary of xDLMS services for LN referencing	73
Table 32 – Summary of xDLMS services for SN referencing	73
Table 33 – ACSE functional units, services and service parameters	77
Table 34 – Use of ciphered / unciphered APDUs	80
Table 35 – xDLMS Conformance block	90
Table 36 – GET service types and APDUs	91
Table 37 – SET service types and APDUs	95
Table 38 – ACTION service types and APDUs	98
Table 39 – Mapping between the GET and the Read services	100
Table 40 – Mapping between the ACTION and the Read services	101
Table 41 – Mapping between the SET and the Write services	105
Table 42 – Mapping between the ACTION and the Write service	106
Table 43 – Mapping between the SET and the UnconfirmedWrite services	108
Table 44 – Mapping between the ACTION and the UnconfirmedWrite services	109
Table 45 – Mapping between the EventNotification and InformationReport services	110
Table B.1 – Conformance block	127
Table B.2 – A-XDR encoding of the xDLMS InitiateRequest APDU	128
Table B.3 – A-XDR encoding of the xDLMS InitiateResponse APDU	129
Table B.4 – BER encoding of the AARQ APDU	132
Table B.5 – Complete AARQ APDU	134
Table B.6 – BER encoding of the AARE APDU	135
Table B.7 – The complete AARE APDU	139
Table C.1 – A-XDR encoding of the xDLMS InitiateRequest APDU	140
Table C.2 – Authenticated encryption of the xDLMS InitiateRequest APDU	141
Table C.3 – BER encoding of the AARQ APDU	142
Table C.4 – A-XDR encoding of the xDLMS InitiateResponse APDU	143
Table C.5 – Authenticated encryption of the xDLMS InitiateResponse APDU	144
Table C.6 – BER encoding of the AARE APDU	145
Table C.7 – BER encoding of the RLRQ APDU	146
Table C.8 – BER encoding of the RLRE APDU	147

Table D.1 – Objects used in the examples	148
Table D.2 – Example: Reading the value of a single attribute without block transfer	149
Table D.3 – Example: Reading the value of a list of attributes without block transfer	150
Table D.4 – Example: Reading the value of a single attribute with block transfer	151
Table D.5 – Example: Reading the value of a list of attributes with block transfer	153
Table D.6 – Example: Writing the value of a single attribute without block transfer	155
Table D.7 – Example: Writing the value of a list of attributes without block transfer	156
Table D.8 – Example: Writing the value of a single attribute with block transfer	158
Table D.9 – Example: Writing the value of a list of attributes with block transfer	160

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 COSEM clients and servers, and defines how to use the DLMS/COSEM application layer in various 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 62056-6-2², 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, Annex C and Annex D (informative) include encoding examples for APDUs.

Annex E (informative) provides an overview of cryptography.

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.

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*

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*

² To be published simultaneously with this part of IEC 62056.

IEC 62056-6-1:—, *Electricity metering data exchange – The DLMS/COSEM suite – Part 6-1: Object Identification System (OBIS)*³

IEC 62056-6-2:—, *Electricity metering data exchange – The DLMS/COSEM suite – Part 6-2: COSEM interface classes*⁴

IEC 62056-8-3:—, *Electricity metering data exchange – The DLMS/COSEM suite – Part 8-3: Communication profile for PLC S-FSK neighbourhood networks*⁵

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*

ISO/IEC 8824-1:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*

ISO/IEC 8825-1:2008, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

FIPS PUB 180-1:2002, *Secure hash standard*

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 800-57:2006, *Recommendation for Key Management – Part 1: General (Revised)*

RFC 1321:1992, Internet Engineering Task Force (IETF). *The MD5 Message-Digest Algorithm*. Edited by R. Rivest (MIT Laboratory for Computer Science and RSA Data Security, Inc.) April 1992. Available from: <http://www.rfc-editor.org/rfc/rfc1321.txt>

RFC 3394:2002, Internet Engineering Task Force (IETF). *Advanced Encryption Standard (AES) Key Wrap Algorithm*. Edited by J. Schaad (Soaring Hawk Consulting) and R. Housley (RSA Laboratories) September 2002. Available from: <http://www.rfc-editor.org/rfc/rfc3394.txt>

RFC 4106:2005, *The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)*

NOTE See also the Bibliography.

³ To be published simultaneously with this part of IEC 62056.

⁴ To be published simultaneously with this part of IEC 62056.

⁵ To be published simultaneously with this part of IEC 62056.