

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**Échange des données de comptage de l'électricité – La suite DLMS/COSEM –
Partie 5-3: Couche application DLMS/COSEM**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2016 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue

Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**Échange des données de comptage de l'électricité – La suite DLMS/COSEM –
Partie 5-3: Couche application DLMS/COSEM**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 17.220; 35.110; 91.140.50

ISBN 978-2-8322-3019-0

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

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 RLREQ 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

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:

DLMS¹ 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 second edition cancels and replaces the first edition of IEC 62056-5-3 published in 2013. It constitutes a technical revision.

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

The text of this standard is based on the following documents:

FDIS	Report on voting
13/1648/FDIS	13/1657/RVD

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

This publication 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.

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 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.

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 62056-6-2:2016, 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, Annex D and Annex E (informative) include encoding examples for APDUs.

Annex F (informative) provides an overview of cryptography.

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

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*

IEC 62056-1-0, *Electricity metering data exchange – The DLMS/COSEM suite – Part 1-0: Smart metering standardisation framework*

IEC 62056-6-1:2015, *Electricity metering data exchange – The DLMS/COSEM suite – Part 6-1: Object Identification System (OBIS)*

IEC 62056-6-2:2016, *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 8824-1:2008, *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)*

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 8649-1:1999 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.

FIPS PUB 180-4:2012, *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)*

The following RFCs are available online from the Internet Engineering Task Force (IETF):
<http://www.ietf.org/rfc/std-index.txt>, <http://www.ietf.org/rfc/>

RFC 1321, *The MD5 Message-Digest Algorithm*. Edited by R. Rivest (MIT Laboratory for Computer Science and RSA Data Security, Inc.) April 1992

RFC 3394, *Advanced Encryption Standard (AES) Key Wrap Algorithm*. Edited by J. Schaad (Soaring Hawk Consulting) and R. Housley (RSA Laboratories) September 2002

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